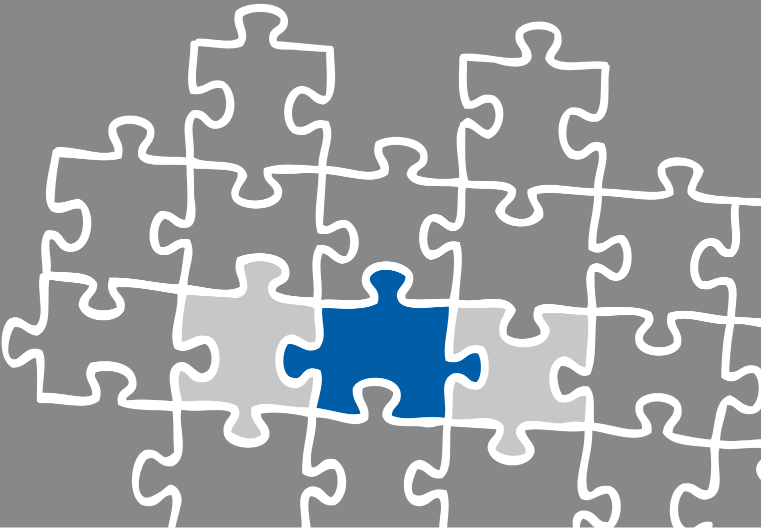
TechNote

XCAPI and Firewalls

June 15, 2011

XCAPI
voiceoverIP



www.te-systems.de

TE-SYSTEMS
competence in e-communications.

Introduction

Current Windows versions protect network interfaces with a firewall which, on the one hand, protects the computer against unauthorised access from outside, and, on the other hand, gives the user a certain degree of control as to which of their programs may access the network. XCAPI VoIP controllers are no exception and are therefore also restricted, mainly with respect to incoming data traffic from the PBX.

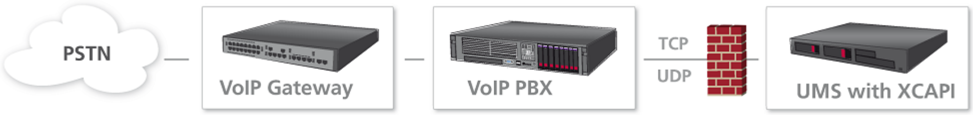
Most XCAPI installations are integrated with a local network which is connected to the Internet via a router. In many cases, routers also act as firewalls, blocking incoming messages from VoIP providers.

XCAPI and Firewalls

For XCAPI to be able to communicate with the PBX or the VoIP provider it has to work around the firewall. The easiest method is to disable the firewall. Although this might be acceptable on the local network, it is definitely something to avoid on the router that connects to the Internet. Due to this, XCAPI supports an option for restricting communication to a certain group of ports, which in turn can be permanently configured on the firewall.

A simple solution that is often seen in productive environments is described below:

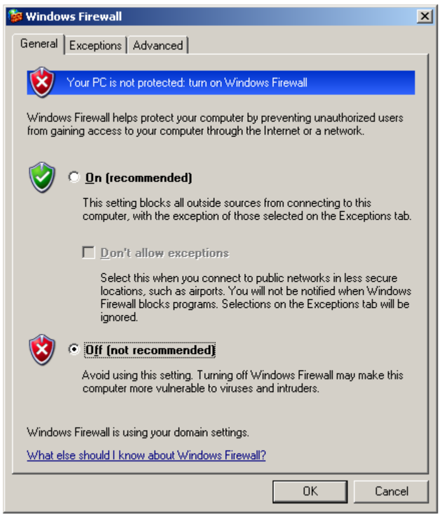
Firewall configuration: XCAPI - PBX



XCAPI is installed on a computer on the LAN and only needs to communicate with a PBX that can be reached on the same sub network. If no security risks are involved, you can disable the firewall on the operating system on which XCAPI is running. This means that all TCP and UDP packets can be freely transferred between XCAPI and the PBX (and to all other network devices). In the Windows Control Panel, you will find the settings for this below `Windows Firewall`.

Option 1: Disable the firewall

The typical solution to firewall problems is to simply disable the firewall. However, attention should be paid to the settings in the `Advanced` tab as these settings usually hamper communication.



Your PC is not protected: turn on Windows Firewall

Windows Firewall helps protect your computer by preventing unauthorized users from gaining access to your computer through the Internet or a network.

○ On (recommended)

This setting blocks all outside sources from connecting to this computer, with the exception of those selected on the Exceptions tab.

□ Don't allow exceptions

Select this when you connect to public networks in less secure locations, such as airports. You will not be notified when Windows Firewall blocks programs. Selections on the Exceptions tab will be ignored.

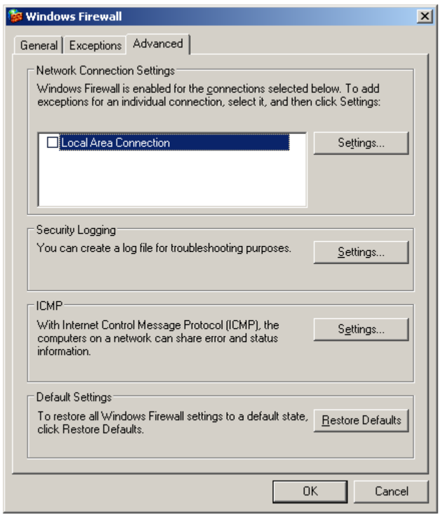
● Off (not recommended)

Avoid using this setting. Turning off Windows Firewall may make this computer more vulnerable to viruses and intruders.

Windows Firewall is using your domain settings.

What else should I know about Windows Firewall?

For this reason, you also need to disable the network interface that XCAPI will be using (e.g. LAN connection 1, etc.) in the `Advanced` tab below `Network connection settings`.



Network Connection Settings

Windows Firewall is enabled for the connections selected below. To add exceptions for an individual connection, select it, and then click Settings:

□ Local Area Connection

Security Logging

You can create a log file for troubleshooting purposes.

ICMP

With Internet Control Message Protocol (ICMP), the computers on a network can share error and status information.

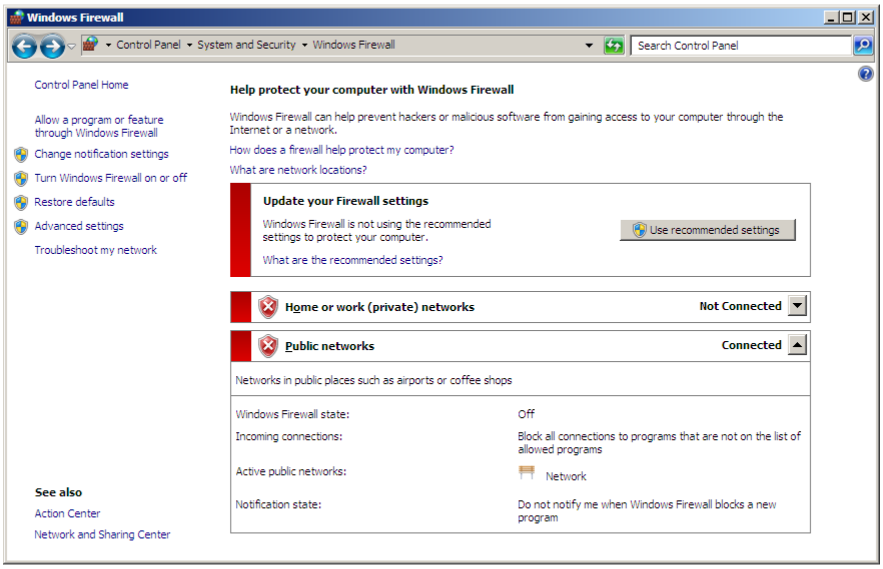
Default Settings

To restore all Windows Firewall settings to a default state, click Restore Defaults.

Pay attention to advanced firewall settings

These settings only apply to systems up to Windows Server 2003 where the default installation disables the firewall - in contrast to other systems - thus avoiding problems.

Also systems up to Windows Server 2008 offers a simple view about disabling the firewall completely.



Windows Firewall

Control Panel ▸ System and Security ▸ Windows Firewall

Search Control Panel

Control Panel Home

Allow a program or feature through Windows Firewall

Change notification settings

Turn Windows Firewall on or off

Restore defaults

Advanced settings

Troubleshoot my network

See also

Action Center

Network and Sharing Center

Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

Update your Firewall settings

Windows Firewall is not using the recommended settings to protect your computer.

What are the recommended settings?

Use recommended settings

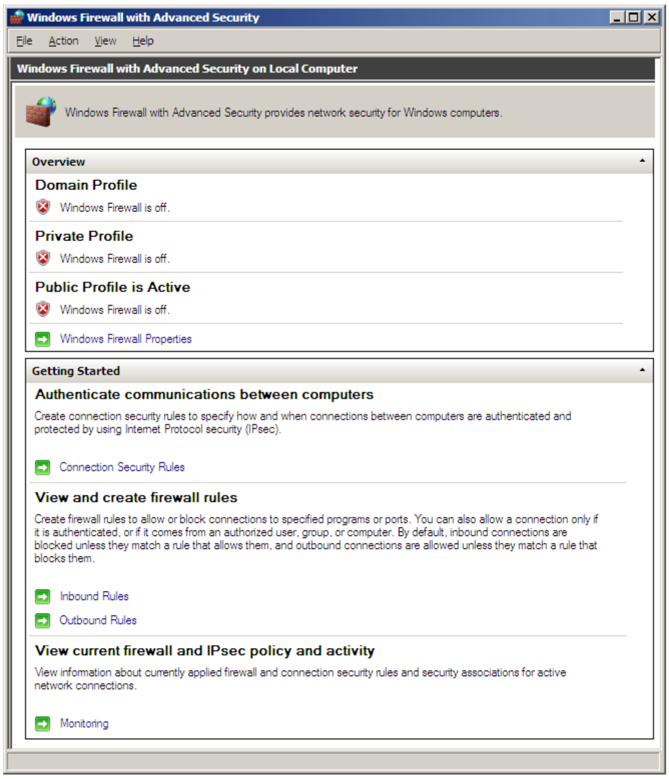
Home or work (private) networks — **Not Connected**

Public networks — **Connected**

Networks in public places such as airports or coffee shops

Windows Firewall state:	Off
Incoming connections:	Block all connections to programs that are not on the list of allowed programs
Active public networks:	Network
Notification state:	Do not notify me when Windows Firewall blocks a new program

Windows Vista or later systems have a different firewall configuration which you also need to take into account. The configuration program for the `Windows Firewall with advanced security` is located in the Windows Control Panel below `Administration`.



Windows Firewall with Advanced Security on Local Computer

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile
Windows Firewall is off.

Private Profile
Windows Firewall is off.

Public Profile is Active
Windows Firewall is off.

Windows Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

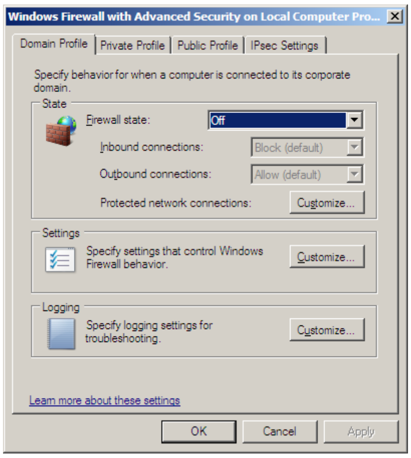
Inbound Rules
Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

Monitoring

Profiles are used here to decide whether or not a connection can be used - depending on which network profile was selected for the network card that XCAPI will be using. You can disable individual or all profiles here in a targeted manner to ensure trouble-free communications.



Windows Firewall with Advanced Security on Local Computer Pro...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

Inbound connections: Block (default)

Outbound connections: Allow (default)

Protected network connections: Customize...

Settings

Specify settings that control Windows Firewall behavior. Customize...

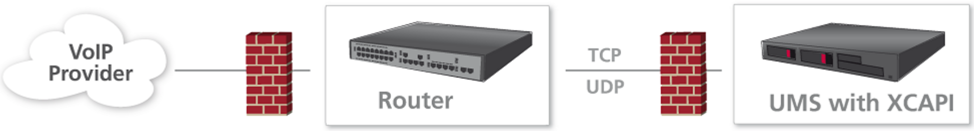
Logging

Specify logging settings for troubleshooting. Customize...

Learn more about these settings

Firewall configuration: XCAPI - router - VoIP provider

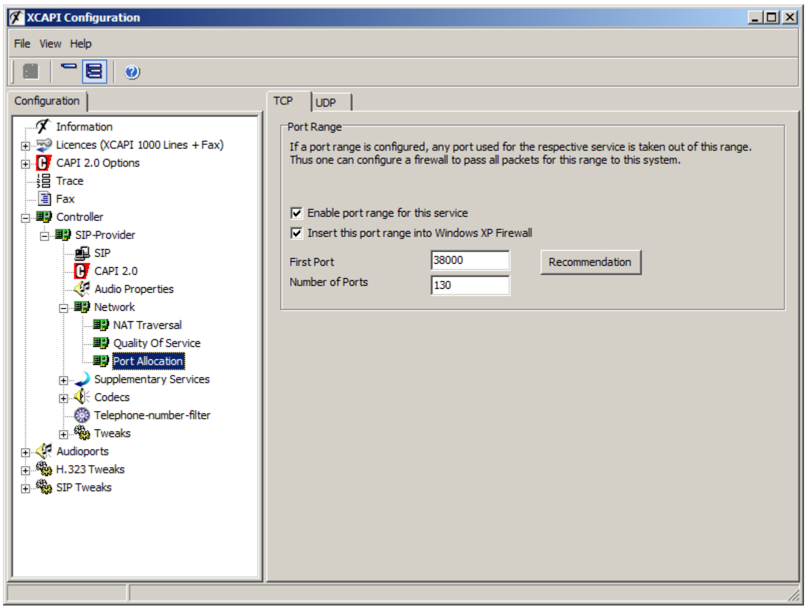
The secure approach, which involves some configuration overhead, can be used both on your intranet and for external connections to VoIP providers. A number of defined ports, which XCAPI needs for signalling and the RTP data, are allowed on the firewall running on the XCAPI computer and/or router. As a result, packets which are essential to VoIP communication can be freely exchanged between XCAPI and the target device while the firewall continues to protect the local network and other operating system functions.



Option 2: Define a port range

Although VoIP signalling uses standard ports in most cases (e.g. `5060` for SIP and `1720` for H.323 signalling), the ports to be used for the RTP data are negotiated between XCAPI and the subscriber during the call set-up. This creates another problem for the firewall administrator, because all ports should actually be enabled under these conditions. It is quite probable that the RTP data will be transmitted via a different port for each call. In order to avoid this issue, you can set up a range of ports for exclusive use by XCAPI in your XCAPI configuration. As a result, the administrator only needs to enable this port range on the firewall, thus reducing security exposure.

In order to define a range of ports for XCAPI, you need to expand the configuration entry for the VoIP controller in the expert view and open the `Port Reservation` menu below `Network`.



Port Range

If a port range is configured, any port used for the respective service is taken out of this range. Thus one can configure a firewall to pass all packets for this range to this system.

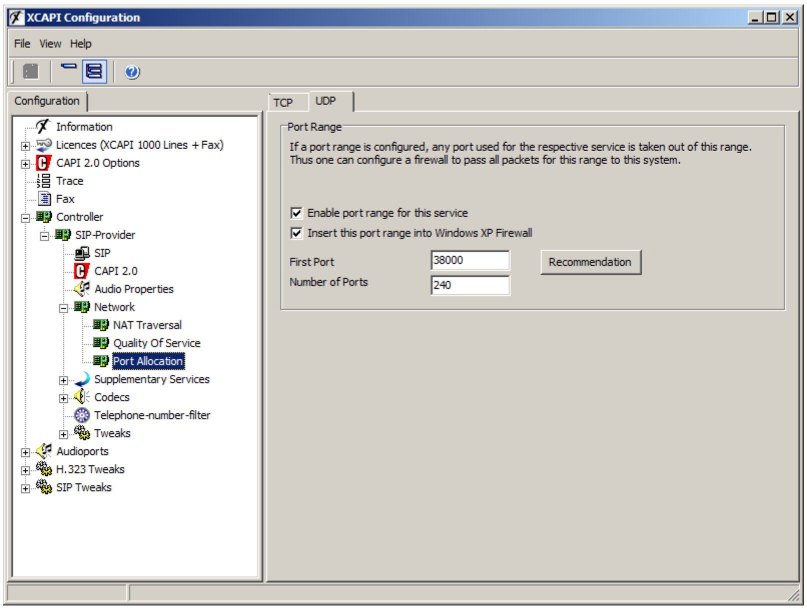
☑ Enable port range for this service

☑ Insert this port range into Windows XP Firewall

First Port: 38000

Number of Ports: 130

You can now enable the TCP and UDP `Port Range` for the protocol in question. A port range is automatically suggested when you press the `Recommendation` button. If the range does not match your planning, you can also define your own range based on the recommendations. Make sure that the range includes the same number of ports as suggested by XCAPI.



Port Range

If a port range is configured, any port used for the respective service is taken out of this range.
Thus one can configure a firewall to pass all packets for this range to this system.

☑ Enable port range for this service

☑ Insert this port range into Windows XP Firewall

First Port: 38000

Number of Ports: 240

Modifying the port settings when adding XCAPI licences

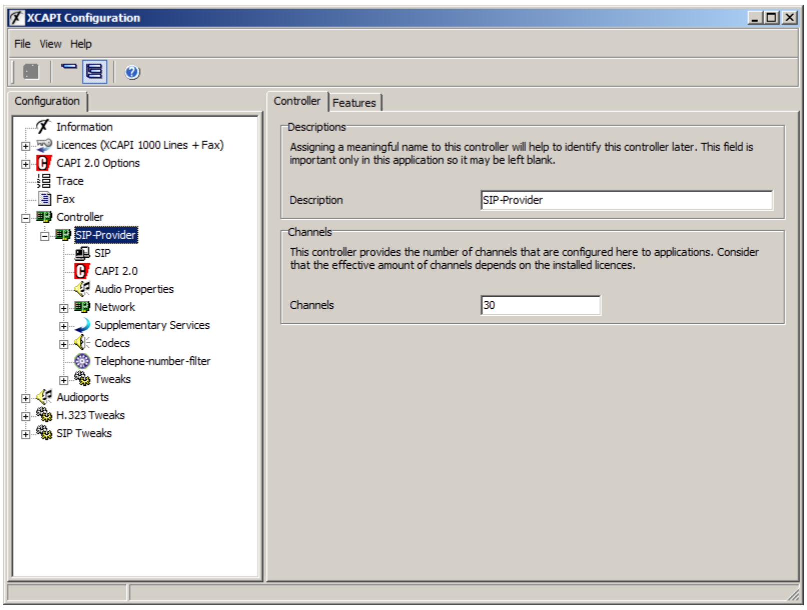
The number of ports is calculated by reference to various controller configuration parameters, such as the number of available channels. The more parallel calls the controller can handle, the greater the number of RTP ports required. You should also bear this in mind if you increase the number of channels at some later stage. In this case, you will also need to increase the number of ports in the port reservation.

After allocating a specific number of ports to XCAPI, you will still need to allow the ports on the firewall. If you are running XCAPI on Windows XP, you can set this up automatically using the configuration tool. In all other cases, you will need to enter these ports manually in your firewall configuration. Remember that you need to allow ports for signalling in addition to the ports reserved for RTP.

Enter defined port area in local Firewall

Here you find a sample configuration of an SIP connection:

We configured a SIP controller for autonomous registration with a SIP provider and parallel use of 30 channels.



Descriptions

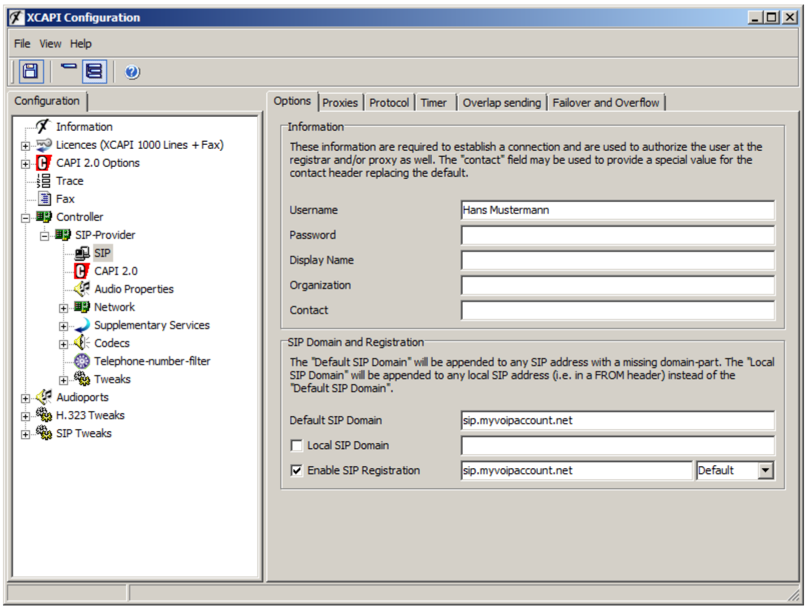
Assigning a meaningful name to this controller will help to identify this controller later. This field is important only in this application so it may be left blank.

Description: SIP-Provider

Channels

This controller provides the number of channels that are configured here to applications. Consider that the effective amount of channels depends on the installed licences.

Channels: 30



Information

These information are required to establish a connection and are used to authorize the user at the registrar and/or proxy as well. The "contact" field may be used to provide a special value for the contact header replacing the default.

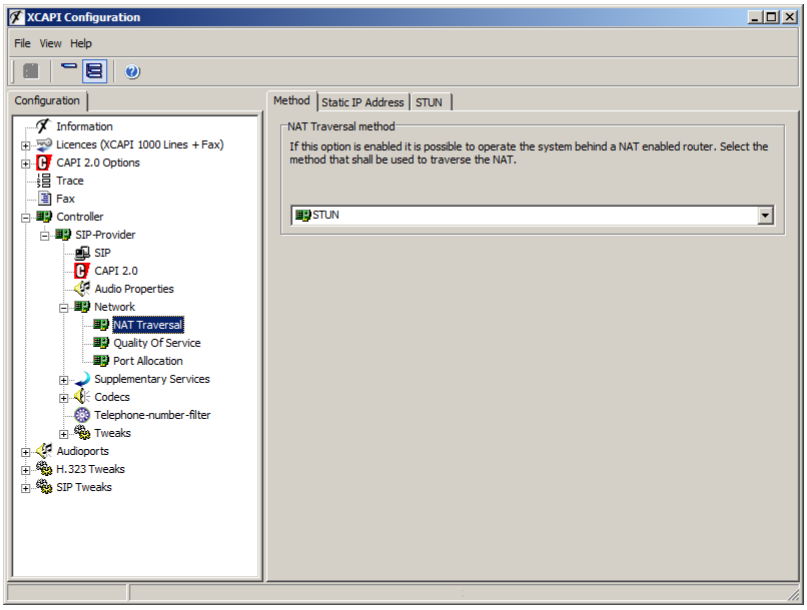
Username: Hans Mustermann
Password:
Display Name:
Organization:
Contact:

SIP Domain and Registration

The "Default SIP Domain" will be appended to any SIP address with a missing domain-part. The "Local SIP Domain" will be appended to any local SIP address (i.e. in a FROM header) instead of the "Default SIP Domain".

Default SIP Domain: sip.myvoipaccount.net
□ Local SIP Domain:
☑ Enable SIP Registration: sip.myvoipaccount.net Default

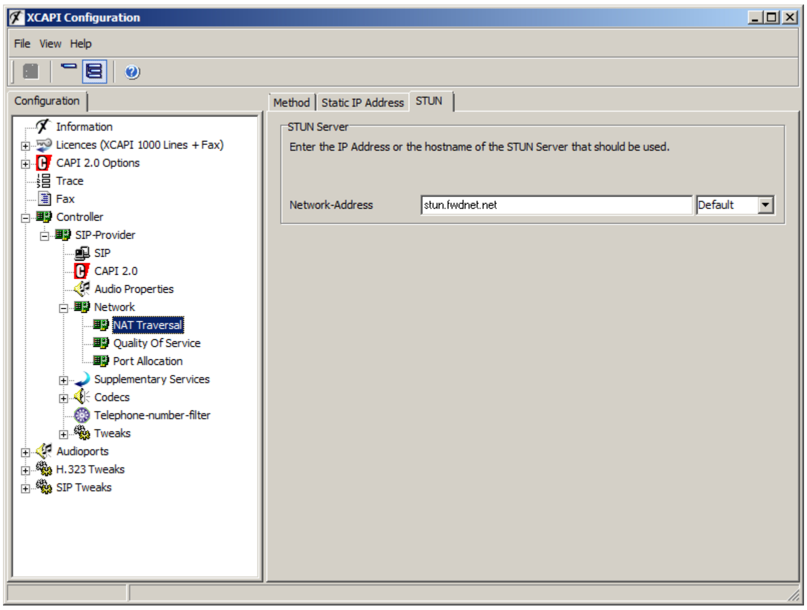
The SIP provider requires the use of a STUN server, because we are on a local network.



NAT Traversal method

If this option is enabled it is possible to operate the system behind a NAT enabled router. Select the method that shall be used to traverse the NAT.

STUN



STUN Server

Enter the IP Address or the hostname of the STUN Server that should be used.

Network-Address: stun.fwdnet.net Default

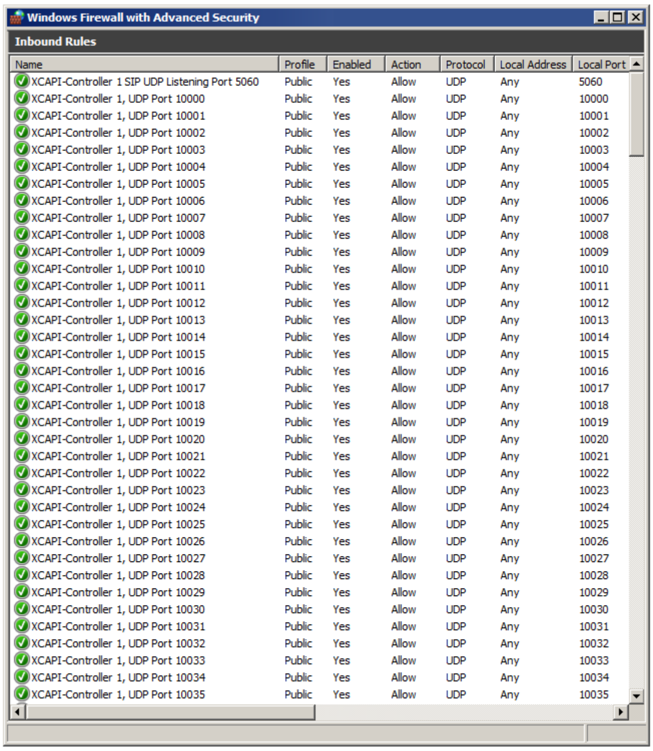
The recommendation for the port reservation begins with the value `10000` as the first port and a total of `100` ports for TCP and `180` ports for UDP. First of all, you should check whether TCP is actually required, because SIP often runs on top of UDP and RTP data are generally transferred via UDP only.

In our example, our SIP provider only supports UDP and do not need to enable any ports for TCP.

Given these circumstances, the following ports are enabled:

- `5060/UDP` for SIP signalling.
- `3478/UDP` for the STUN server.
- `10000-10179/UDP` (a total of `180 ports`) from the port reservation.

These ports must initially be allowed on the XCAPI computer's local firewall so that the packets can reach XCAPI. Furthermore, the router that connects the network to the Internet has to be configured to implement port forwarding for individual ports to the corresponding destination ports at the XCAPI IP address.



Name	Profile	Enabled	Action	Protocol	Local Address	Local Port
XCAPI-Controller 1 SIP UDP Listening Port 5060	Public	Yes	Allow	UDP	Any	5060
XCAPI-Controller 1, UDP Port 10000	Public	Yes	Allow	UDP	Any	10000
XCAPI-Controller 1, UDP Port 10001	Public	Yes	Allow	UDP	Any	10001
XCAPI-Controller 1, UDP Port 10002	Public	Yes	Allow	UDP	Any	10002
XCAPI-Controller 1, UDP Port 10003	Public	Yes	Allow	UDP	Any	10003
XCAPI-Controller 1, UDP Port 10004	Public	Yes	Allow	UDP	Any	10004
XCAPI-Controller 1, UDP Port 10005	Public	Yes	Allow	UDP	Any	10005
XCAPI-Controller 1, UDP Port 10006	Public	Yes	Allow	UDP	Any	10006
XCAPI-Controller 1, UDP Port 10007	Public	Yes	Allow	UDP	Any	10007
XCAPI-Controller 1, UDP Port 10008	Public	Yes	Allow	UDP	Any	10008
XCAPI-Controller 1, UDP Port 10009	Public	Yes	Allow	UDP	Any	10009
XCAPI-Controller 1, UDP Port 10010	Public	Yes	Allow	UDP	Any	10010
XCAPI-Controller 1, UDP Port 10011	Public	Yes	Allow	UDP	Any	10011
XCAPI-Controller 1, UDP Port 10012	Public	Yes	Allow	UDP	Any	10012
XCAPI-Controller 1, UDP Port 10013	Public	Yes	Allow	UDP	Any	10013
XCAPI-Controller 1, UDP Port 10014	Public	Yes	Allow	UDP	Any	10014
XCAPI-Controller 1, UDP Port 10015	Public	Yes	Allow	UDP	Any	10015
XCAPI-Controller 1, UDP Port 10016	Public	Yes	Allow	UDP	Any	10016
XCAPI-Controller 1, UDP Port 10017	Public	Yes	Allow	UDP	Any	10017
XCAPI-Controller 1, UDP Port 10018	Public	Yes	Allow	UDP	Any	10018
XCAPI-Controller 1, UDP Port 10019	Public	Yes	Allow	UDP	Any	10019
XCAPI-Controller 1, UDP Port 10020	Public	Yes	Allow	UDP	Any	10020
XCAPI-Controller 1, UDP Port 10021	Public	Yes	Allow	UDP	Any	10021
XCAPI-Controller 1, UDP Port 10022	Public	Yes	Allow	UDP	Any	10022
XCAPI-Controller 1, UDP Port 10023	Public	Yes	Allow	UDP	Any	10023
XCAPI-Controller 1, UDP Port 10024	Public	Yes	Allow	UDP	Any	10024
XCAPI-Controller 1, UDP Port 10025	Public	Yes	Allow	UDP	Any	10025
XCAPI-Controller 1, UDP Port 10026	Public	Yes	Allow	UDP	Any	10026
XCAPI-Controller 1, UDP Port 10027	Public	Yes	Allow	UDP	Any	10027
XCAPI-Controller 1, UDP Port 10028	Public	Yes	Allow	UDP	Any	10028
XCAPI-Controller 1, UDP Port 10029	Public	Yes	Allow	UDP	Any	10029
XCAPI-Controller 1, UDP Port 10030	Public	Yes	Allow	UDP	Any	10030
XCAPI-Controller 1, UDP Port 10031	Public	Yes	Allow	UDP	Any	10031
XCAPI-Controller 1, UDP Port 10032	Public	Yes	Allow	UDP	Any	10032
XCAPI-Controller 1, UDP Port 10033	Public	Yes	Allow	UDP	Any	10033
XCAPI-Controller 1, UDP Port 10034	Public	Yes	Allow	UDP	Any	10034
XCAPI-Controller 1, UDP Port 10035	Public	Yes	Allow	UDP	Any	10035

Enter defined port area on global firewall

XCAPI now notifies the SIP provider during the call set-up that the RTP data can be sent to one of the 180 ports between 10000 and 10179. The router accepts the RTP packets and forwards them to XCAPI on the local network.

These facts make it much easier to troubleshoot firewall-related problems:

If you only allow port 5060, which will mean that signalling between XCAPI and the provider works, the audio data may only be audible at one end for outgoing calls from XCAPI. Your local firewall might allow the data from XCAPI to pass through the local firewall and the firewall on the router in the direction of the provider, but the reverse direction - from the provider to XCAPI - is blocked by the router. If you observe this phenomenon, you should recheck the configuration of all the firewalls involved.

Exclusion of Liability

Copyright © 2011 TE-SYSTEMS GmbH

The information contained in this document was correct at the time of writing. TE-SYSTEMS GmbH reserves the right to make any alterations without prior notice.

The utmost care was applied during the compilation of texts and images, as well as during the creation of the software. Nevertheless, no responsibility can be taken for the content being accurate, up to date or complete, nor for the efficient or error-free operation of the software for a particular purpose. Therefore, TE-SYSTEMS GmbH cannot be held liable for any damages resulting directly or indirectly from the use of this document.

Trademarks

All names of products or services used are trademarks or registered trademarks (also without specified indication) of the respective private or legal persons and are therefore subject to legal regulations.

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

Managing Directors Andreas Geiger
Oliver Körber

Address Max-von-Laue-Weg 19
38448 Wolfsburg
Germany

Tel. +49 5363 8195-0
Fax +49 5363 8195-999

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