Configuring XiVO with Untangle Firewall

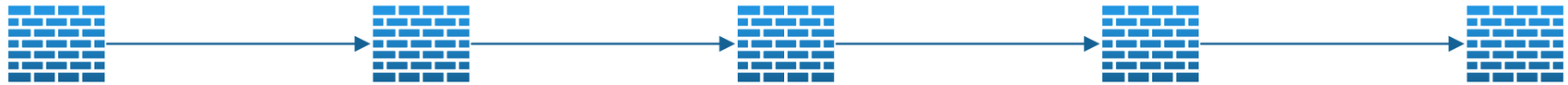
How to Successfully Firewall XiVO with Untangle

Written by Scott McCarthy & Sylvain Boily
www.smsitgroup.com

SMS IT Group
www.smsitgroup.com

XiVO Server w/Firewall Configuration (Untangle)

April 29, 2016



Step 1: SELECT IP

Select an External IP You Will Dedicate to The XiVO Server. Must Be a STATIC EXT IP.

For this example, I am using 66.172.12.2

Step 2: PORT FORWARDING RULES

Setup 2 port forwarding rules that forward in port 5060 UDP and 10000-20000 UDP

Step 3: NAT RULE

Add a NAT rule That tells Untangle To always send XiVO traffic out Your static IP. Our Example IP is 66.172.12.2

I would add a NAT RULE to tell Untangle to always send any traffic from XiVO through 66.172.12.2

Step 4: BYPASS RULES

By default, Untangle reads through ALL traffic and inspects it which ends up screwing up SIP traffic. To stop this, we add bypass rules to tell the firewall NOT to inspect and change the traffic

Step 5 SIP HELPER

Make sure SIP Helper and other Untangle options are configured properly

Untangle NAT RULES

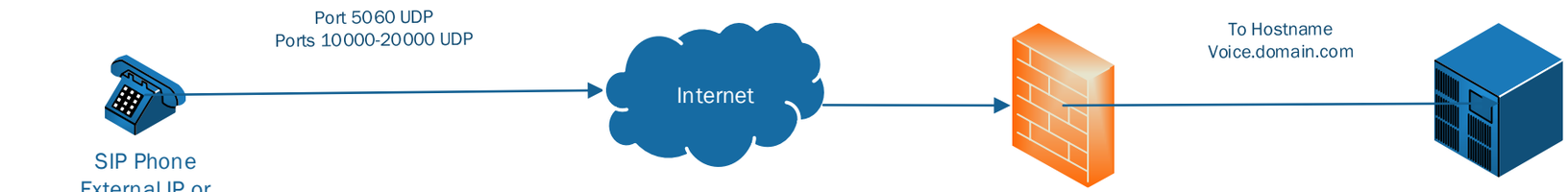
Untangle: CONFIG:NAT Rules: ADD

In order for Untangle to successfully process the traffic, you need to make sure you have a PORT FORWARD RULE that allows the traffic in but you also need a NAT rule to make sure the traffic goes out the CORRECT IP. You need to dedicate an IP to XiVO for this to work. For example, let's say I have a block of Ips that are 66.172.12.1 to .50. I would take 66.172.12.2 and use that for my firewall IP for my XiVO rules.

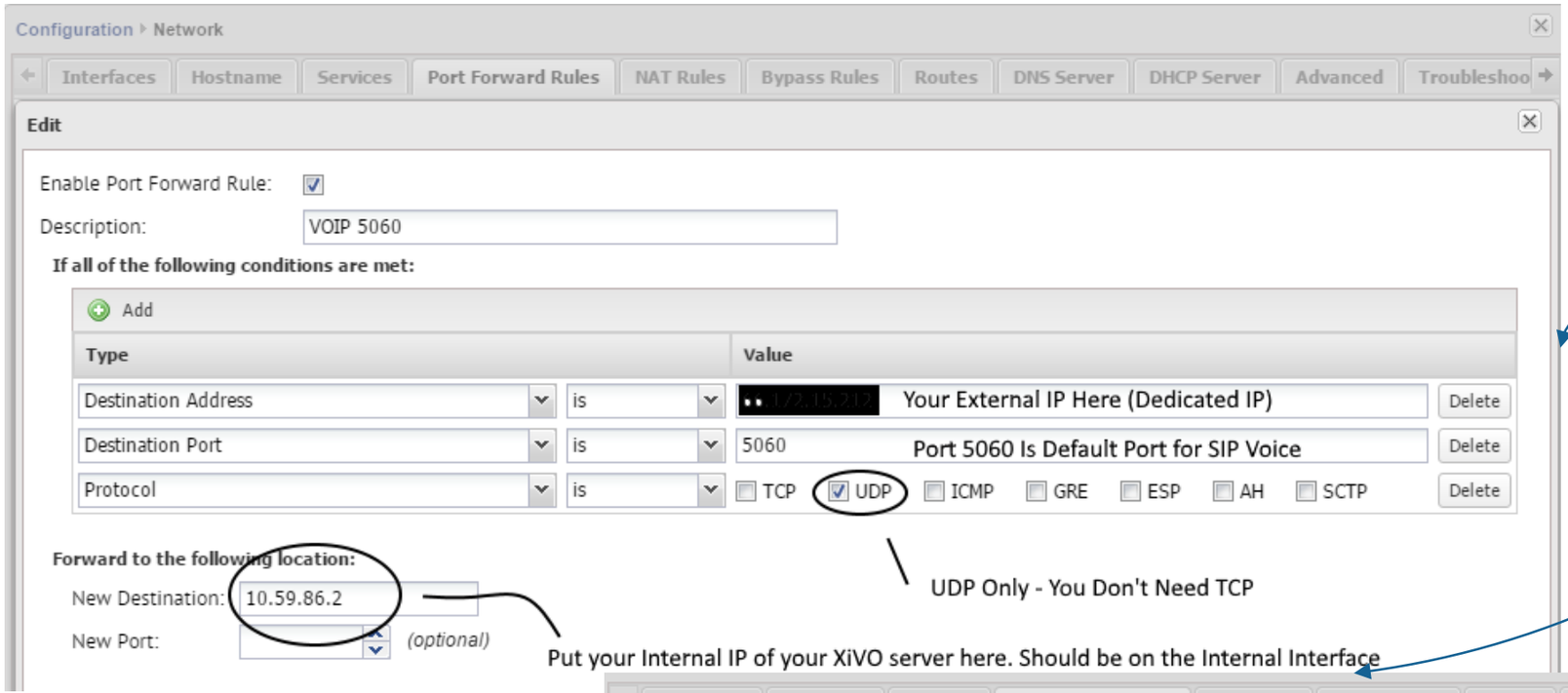
Untangle Firewall

SMS IT Group

www.smsitgroup.com



XiVO Server w/Firewall Configuration (Untangle)

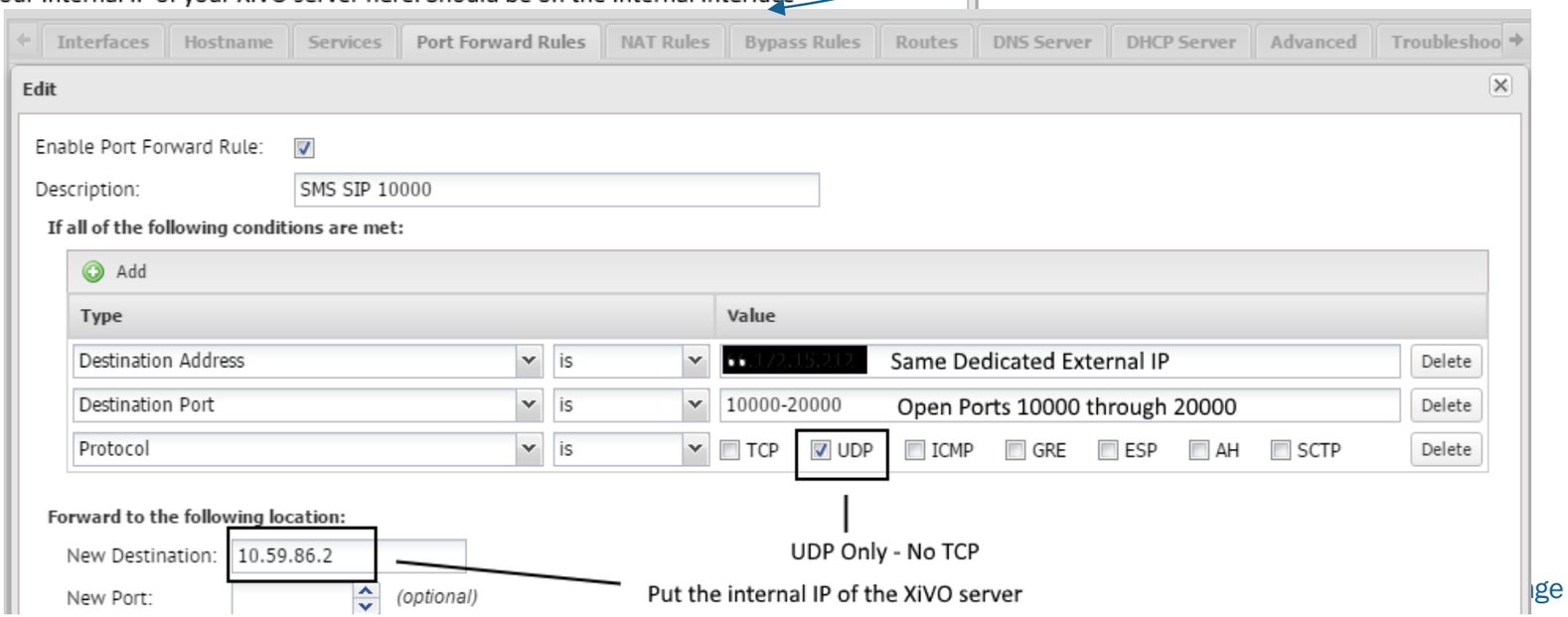


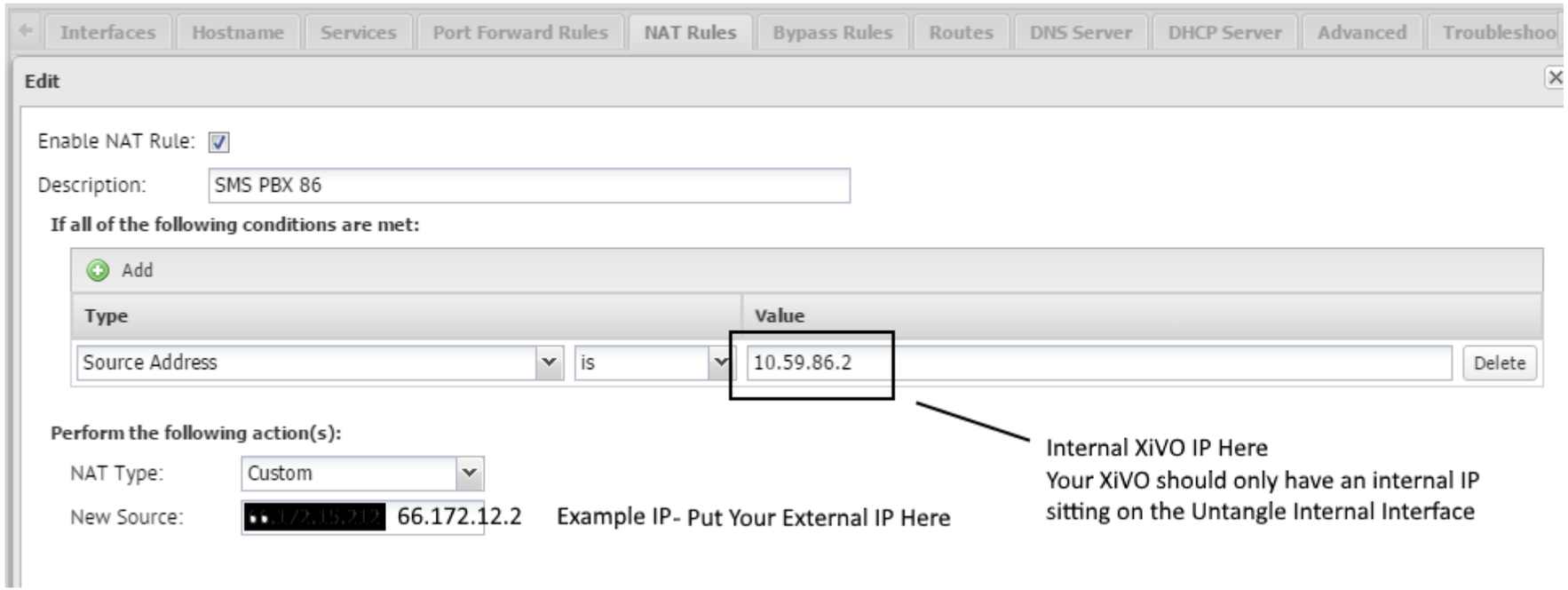
Define 2 Rules in Untangle in the PORT FORWARDING RULES under NETWORK

Untangle PORT FORWARD RULES
(Untangle: CONFIG:PORT FORWARD RULES:ADD +

Login to your Untangle interface and go to CONFIG or NETWORK config depending on version. Then you want to 1st create 2 rules in your PORT FORWARDING RULES. 1st rule is for port 5060 SIP and the 2nd rule is for 10000-20000 ports for phones to connect.

Untangle Firewall



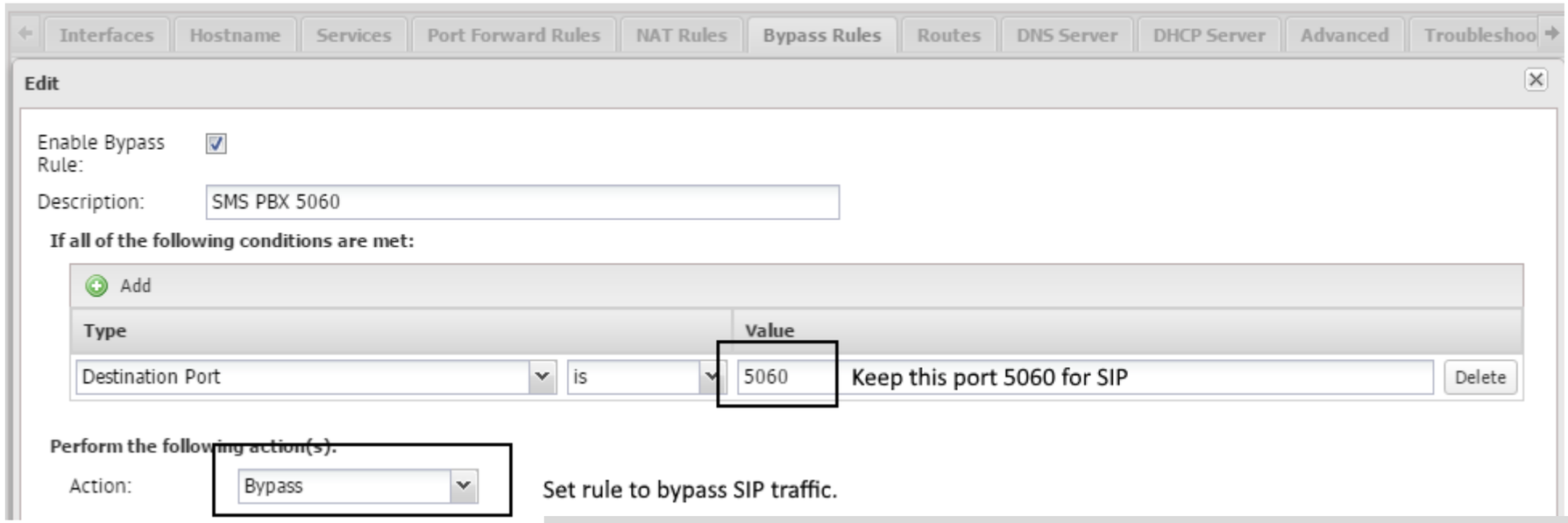


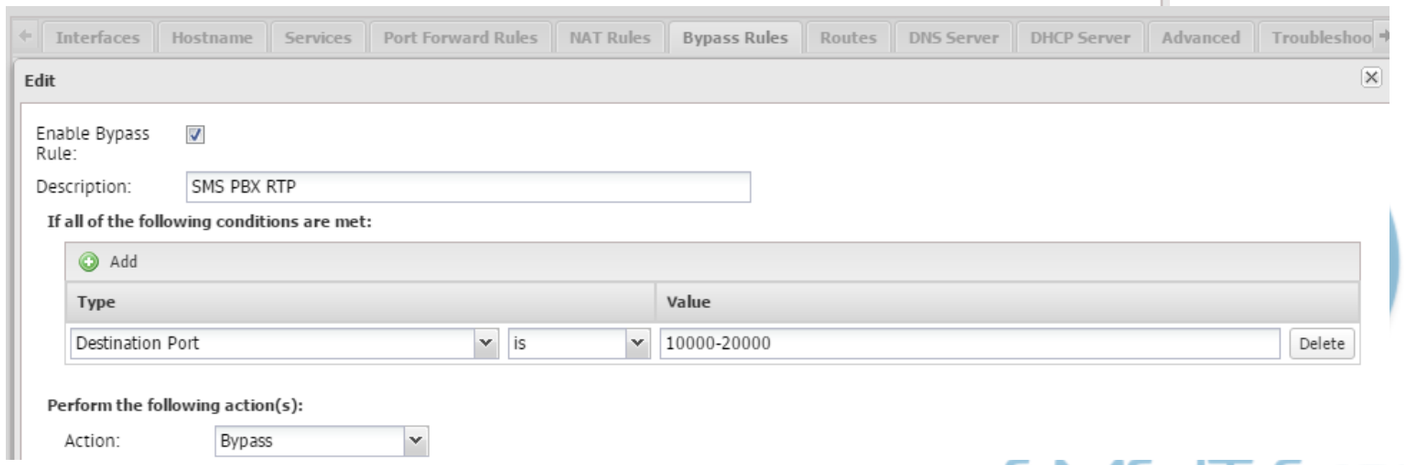
Untangle NAT RULES
(Untangle: CONFIG:NAT RULES

Go to NAT RULES and add 1 rule to tell Untangle to send the traffic out the same external IP every time. In this example, my external IP is 66.172.12.2 and my XiVO server is 10.59.86.2.

Untangle Firewall

SMS IT Group
www.smsitgroup.com





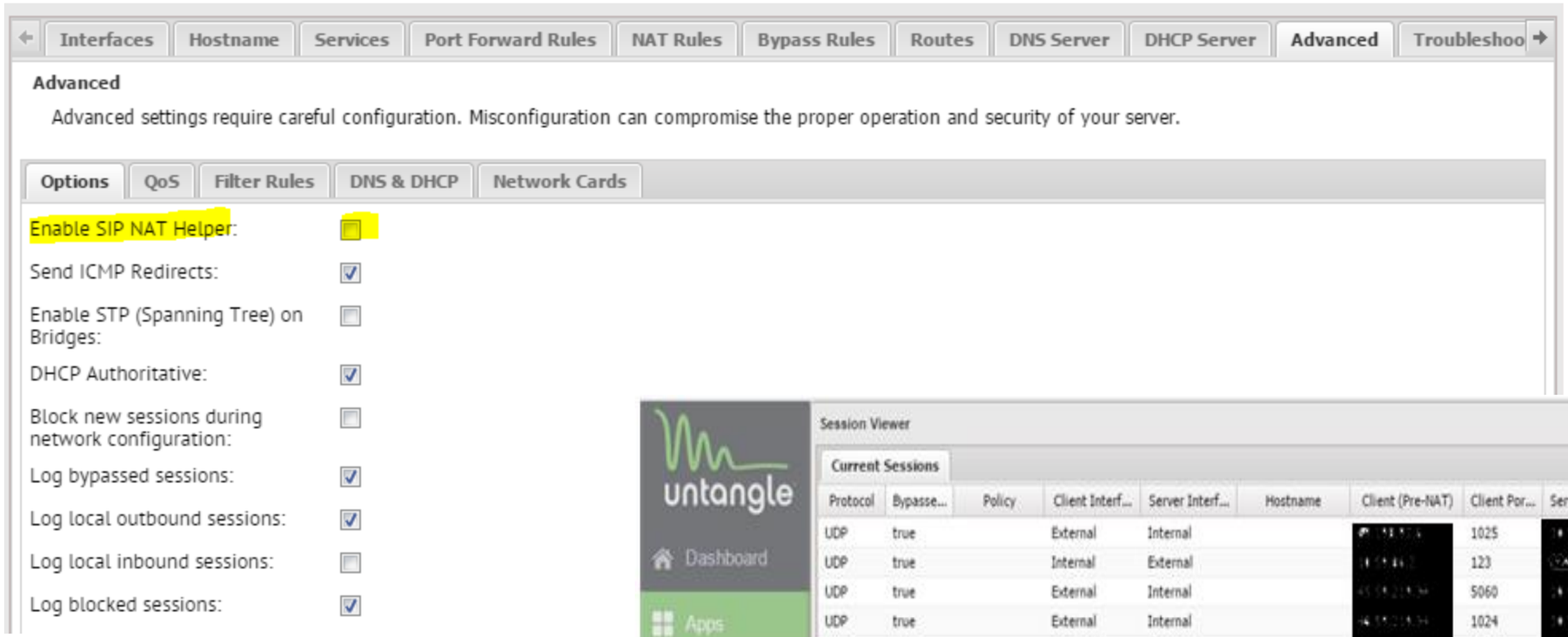
Untangle BYPASS
(Untangle: CONFIG:BYPASS RULES

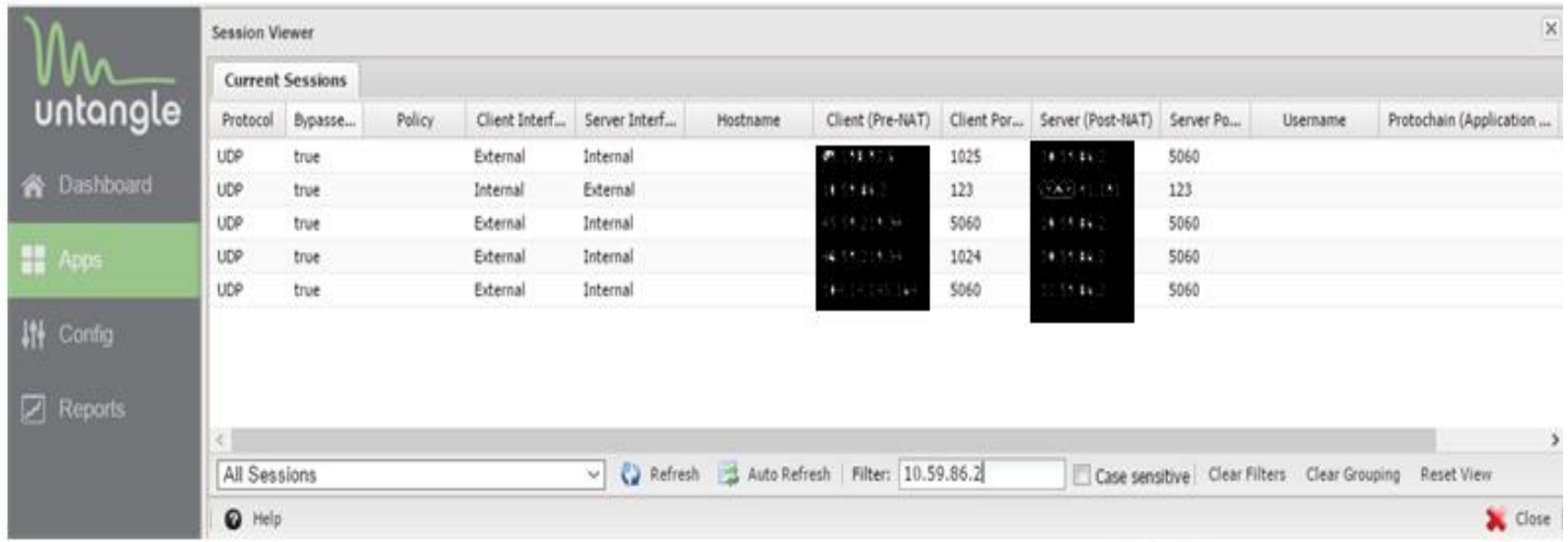
Next, setup a bypass rule that tell Untangle to bypass all traffic on port 5060.

Add a 2nd rule for ports 10000-20000

Untangle Firewall

SMS IT Group
www.smsitgroup.com





Untangle SIP HELPER
(Untangle: CONFIG:ADVANCED

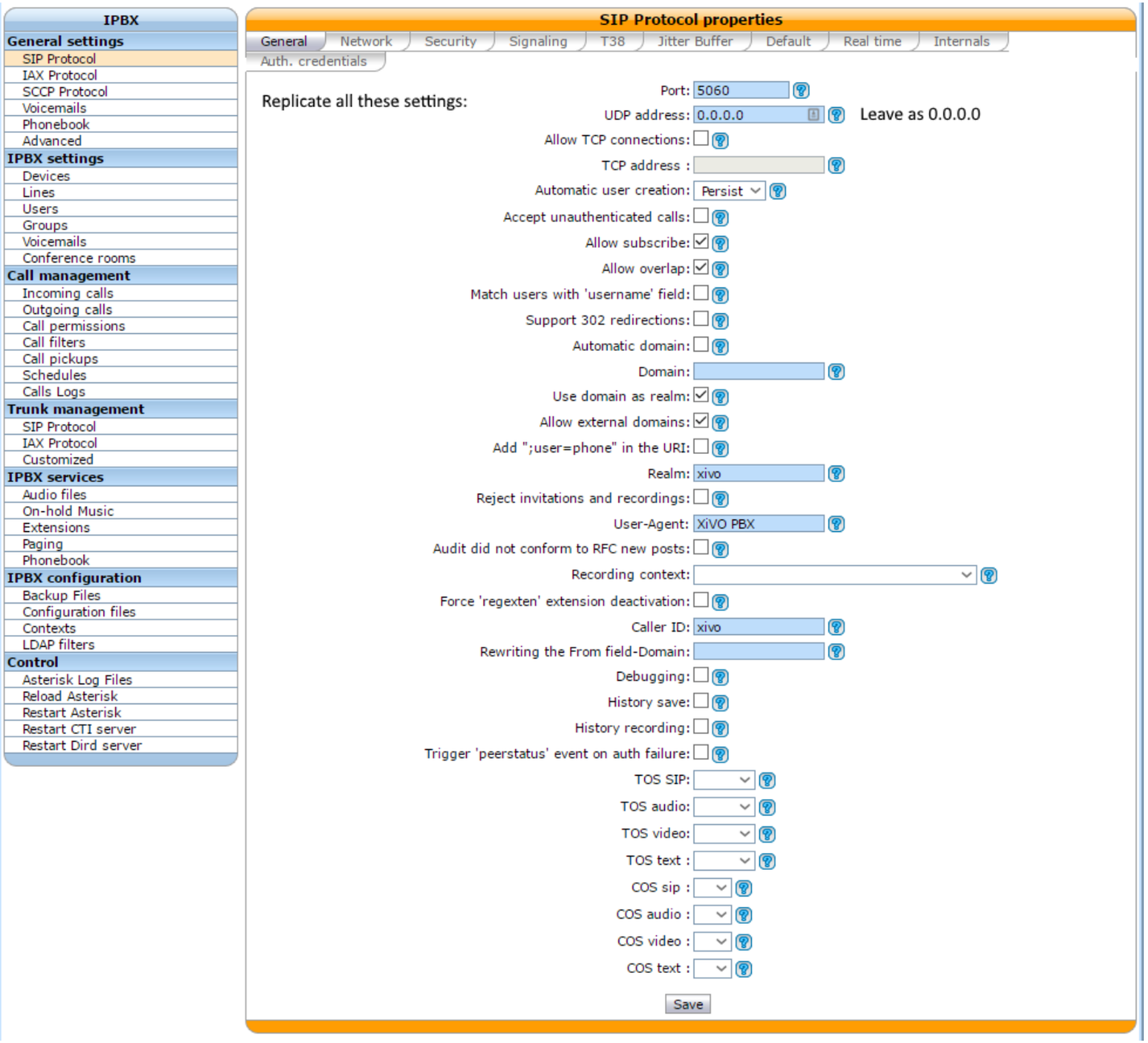
Finally, you need to make sure SIP HELPER is turned OFF. When you make this change, make sure you reboot the firewall to clear out the translation tables

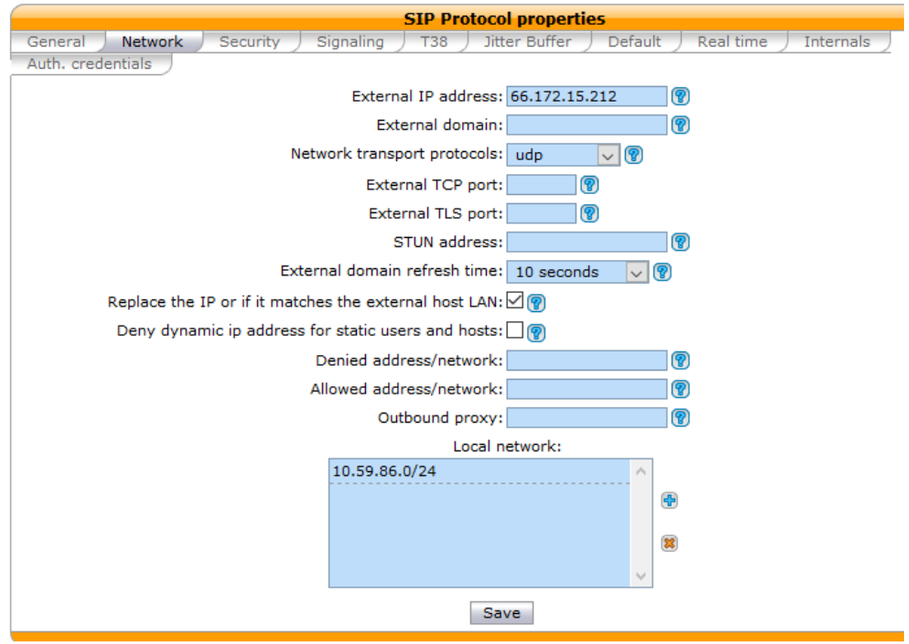
Untangle Firewall

Check To See If It Works

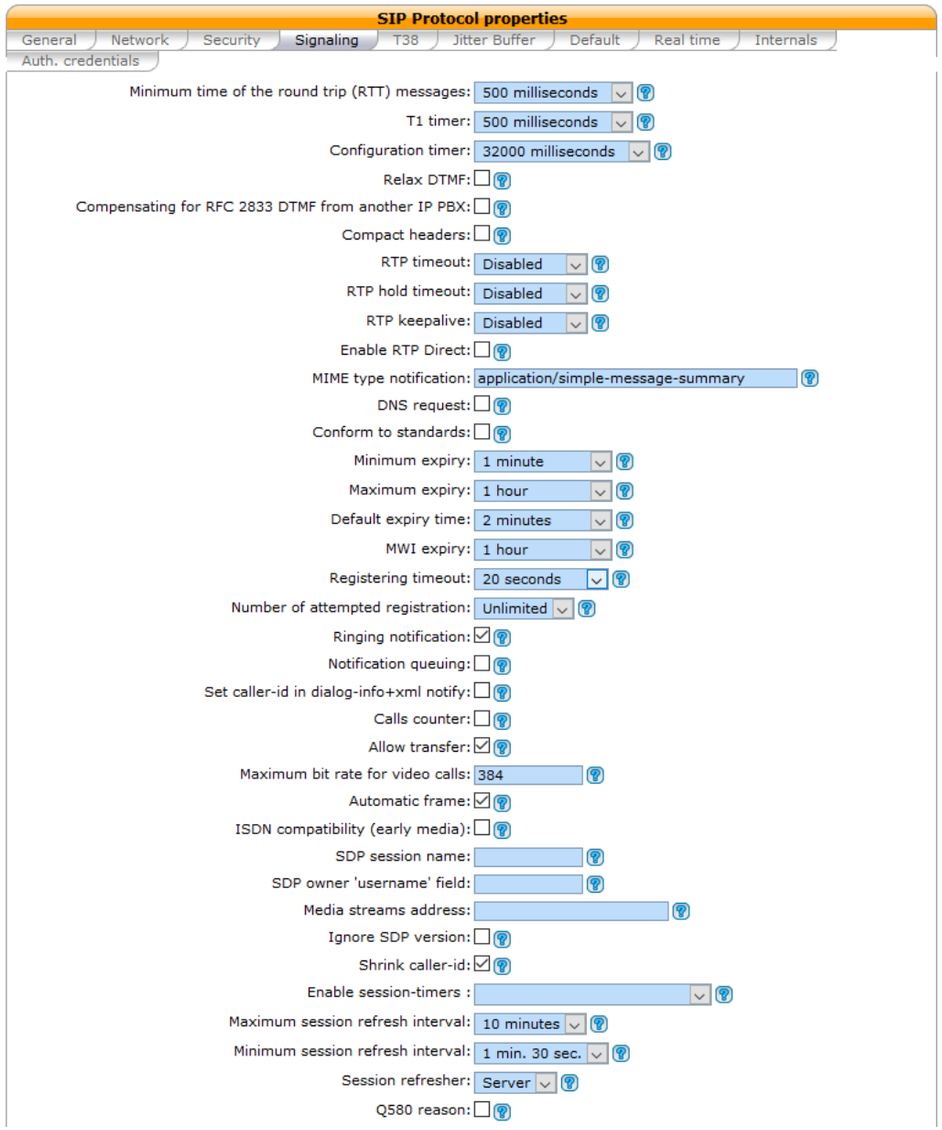
You can check to see if your settings work by going to the SESSION VIEWER in Untangle and enter your INTERNAL IP (IE. 10.59.86.2) and you will see all the traffic in and out to the XiVO server. Make sure all rules show BYPASS TRUE and are NOT being blocked. If they are, you have a configuration setting incorrect.

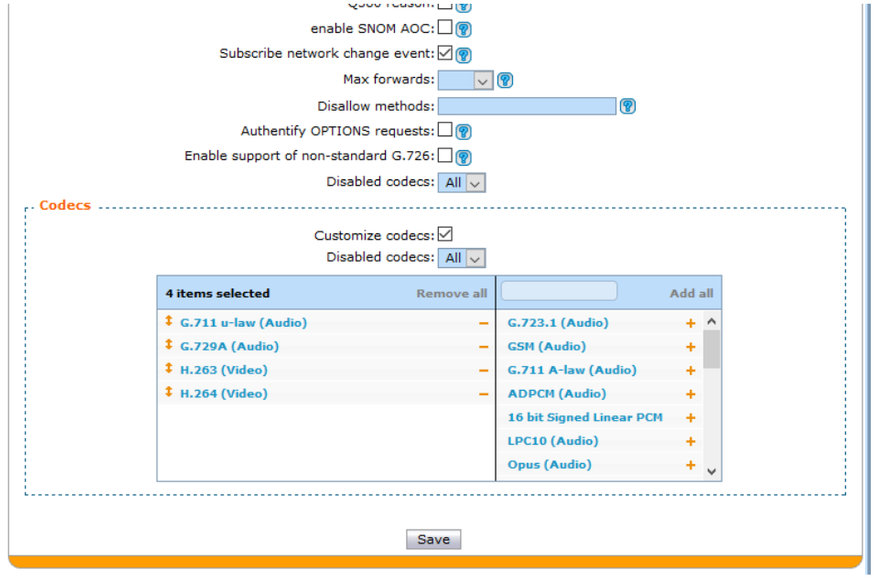
SMS IT Group
www.smsitgroup.com

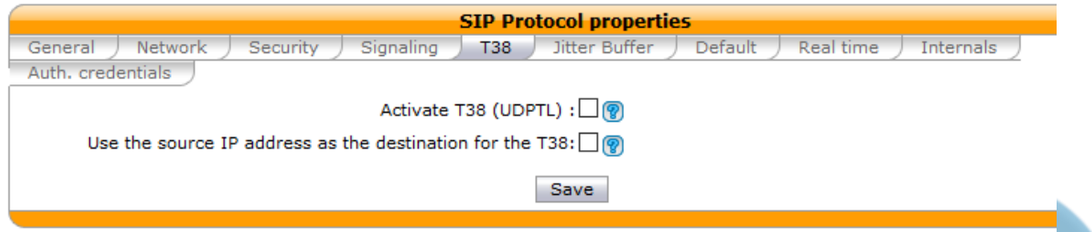


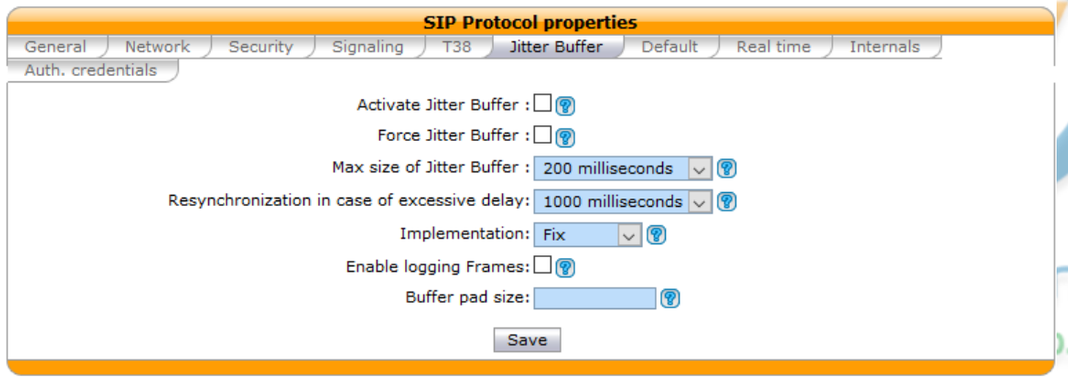


Go to SERVICES:IPBX:GENERAL SETTINGS:SIP PROTOCOL
In this section, follow the settings on this screen. Pay close attention when to enter your external or internal IP and make sure you get the NAT settings correct. One setting can break everything.


SIP Protocol properties
General
Network
Security
Signaling
T38
Jitter Buffer
Default
Real time
Internals
Auth. credentials
Minimum time of the round trip (RTT) messages: 500 milliseconds
T1 timer: 500 milliseconds
Configuration timer: 32000 milliseconds
Relax DTMF:
Compensating for RFC 2833 DTMF from another IP PBX:
Compact headers:
RTP timeout: Disabled
RTP hold timeout: Disabled
RTP keepalive: Disabled
Enable RTP Direct:
MIME type notification: application/simple-message-summary
DNS request:
Conform to standards:
Minimum expiry: 1 minute
Maximum expiry: 1 hour
Default expiry time: 2 minutes
MWI expiry: 1 hour
Registering timeout: 20 seconds
Number of attempted registration: Unlimited
Ringing notification:
Notification queuing:
Set caller-id in dialog-info+xml notify:
Calls counter:
Allow transfer:
Maximum bit rate for video calls: 384
Automatic frame:
ISDN compatibility (early media):
SDP session name:
SDP owner 'username' field:
Media streams address:
Ignore SDP version:
Shrink caller-id:
Enable session-timers :
Maximum session refresh interval: 10 minutes
Minimum session refresh interval: 1 min. 30 sec.
Session refresher: Server
Q580 reason:


enable SNOM AOC:
Subscribe network change event:
Max forwards:
Disallow methods:
Authentify OPTIONS requests:
Enable support of non-standard G.726:
Disabled codecs: All
Codecs
Customize codecs:
Disabled codecs: All
4 items selected
Remove all
Add all
G.711 u-law (Audio)
G.729A (Audio)
H.263 (Video)
H.264 (Video)
G.723.1 (Audio)
GSM (Audio)
G.711 A-law (Audio)
ADPCM (Audio)
16 bit Signed Linear PCM
LPC10 (Audio)
Opus (Audio)
Save


SIP Protocol properties
General
Network
Security
Signaling
T38
Jitter Buffer
Default
Real time
Internals
Auth. credentials
Activate T38 (UDPTL) :
Use the source IP address as the destination for the T38:
Save


SIP Protocol properties
General
Network
Security
Signaling
T38
Jitter Buffer
Default
Real time
Internals
Auth. credentials
Activate Jitter Buffer :
Force Jitter Buffer :
Max size of Jitter Buffer : 200 milliseconds
Resynchronization in case of excessive delay: 1000 milliseconds
Implementation: Fix
Enable logging Frames:
Buffer pad size:
Save

SIP Protocol properties

General | Network | Security | Signaling | T38 | Jitter Buffer | Default | Real time | Internals

Auth. credentials

Context:
NAT: Yes (force rport + comedia)
DTMF: RFC 2833
Monitoring: No
Qualify frequency: 1 minute
Qualify gap: 100 milliseconds
Num. of peers qualified at the same time (per group): 1
Client code:
Inband RING event: Never
Languages: en_US
On-Hold Music: default
Music waiting on an outgoing call:
Voicemail extension: *98
Trust the Remote-Party-ID:
Send the Remote-Party-ID: PAI
Redirect media streams: No
Insecure: No
Text support:
Video support: Yes

Save

SIP Protocol properties

General | Network | Security | Signaling | T38 | Jitter Buffer | Default | Real time | Internals

Auth. credentials

Username	Password type	Password	Realm
No credentials			

Save

SIP Protocol properties

General | Network | Security | Signaling | T38 | Jitter Buffer | Default | Real time | Internals

Auth. credentials

Cache accounts:
Cache update:
Ignore registration expiration:
Save the system name when recording:
Automatic cache clearing: No

Save

SIP Protocol properties

General | Network | Security | Signaling | T38 | Jitter Buffer | Default | Real time | Internals

Auth. credentials

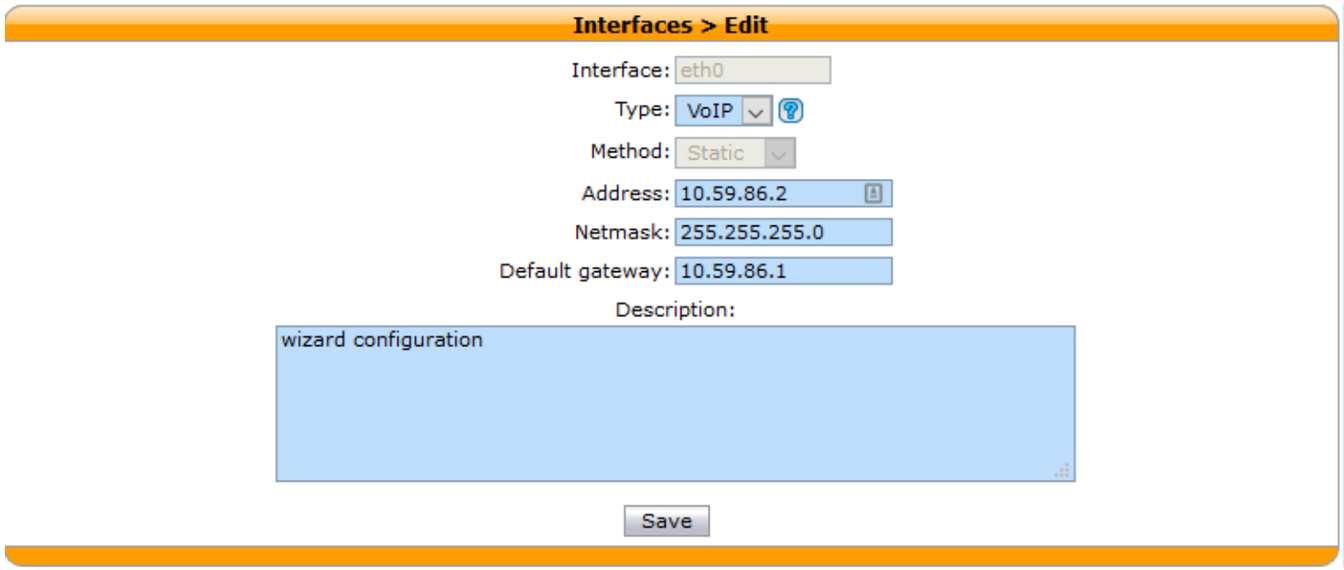
Users hash size:
Peers hash size:
Dialogs hash size:

Save

SMS IT Group
www.smsitgroup.com

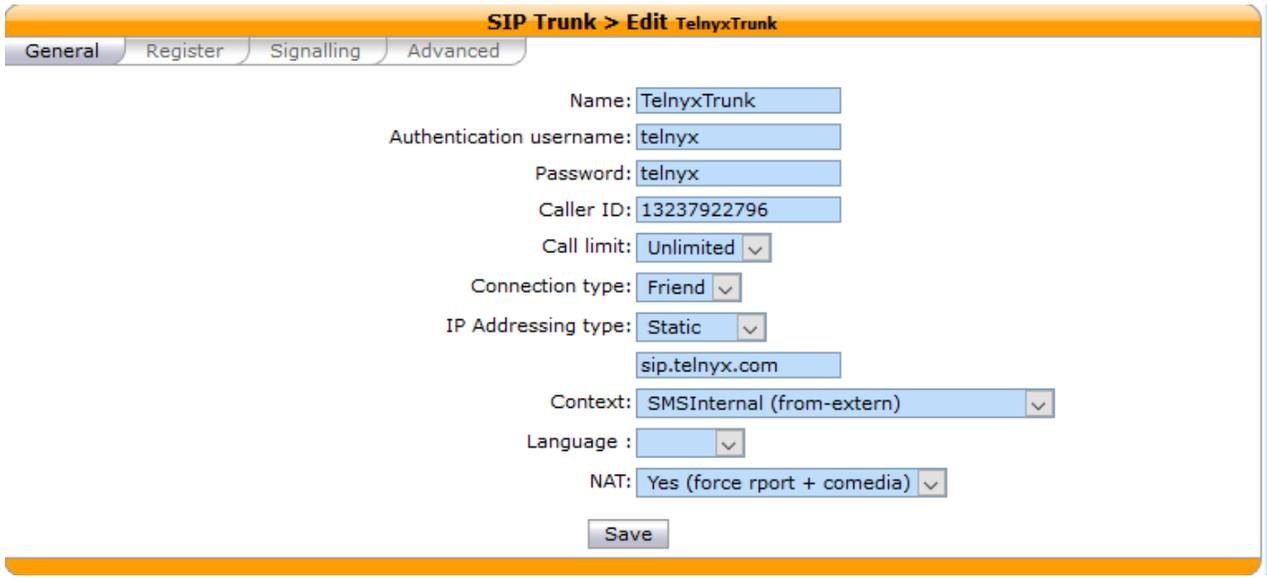
Go to CONFIGURATION:NETWORK:Interfaces

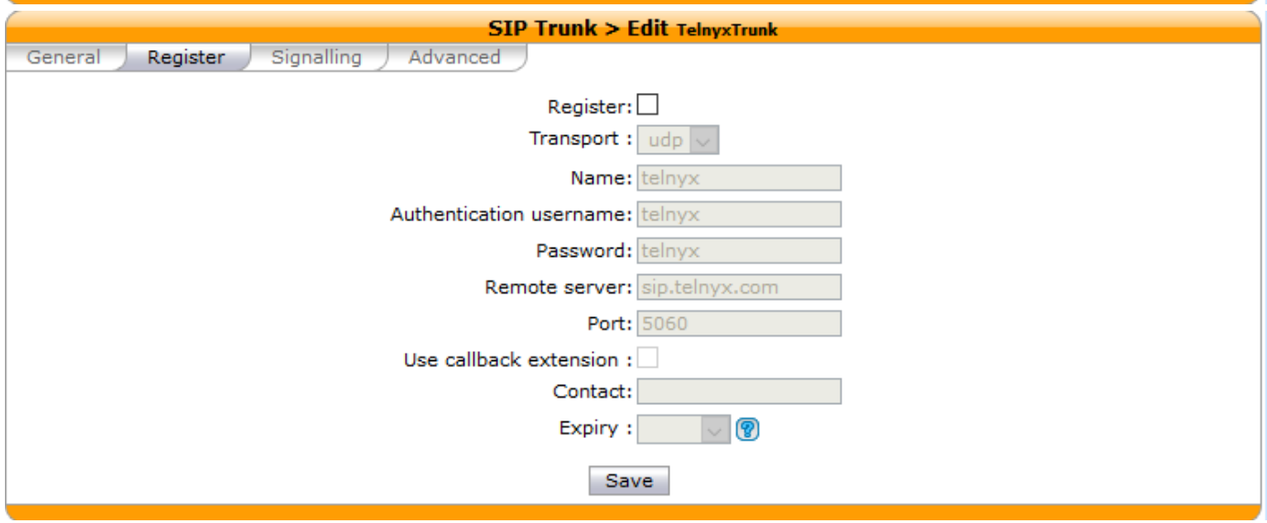
In this section, make sure you use the internal IP of the XiVO server – NOT external

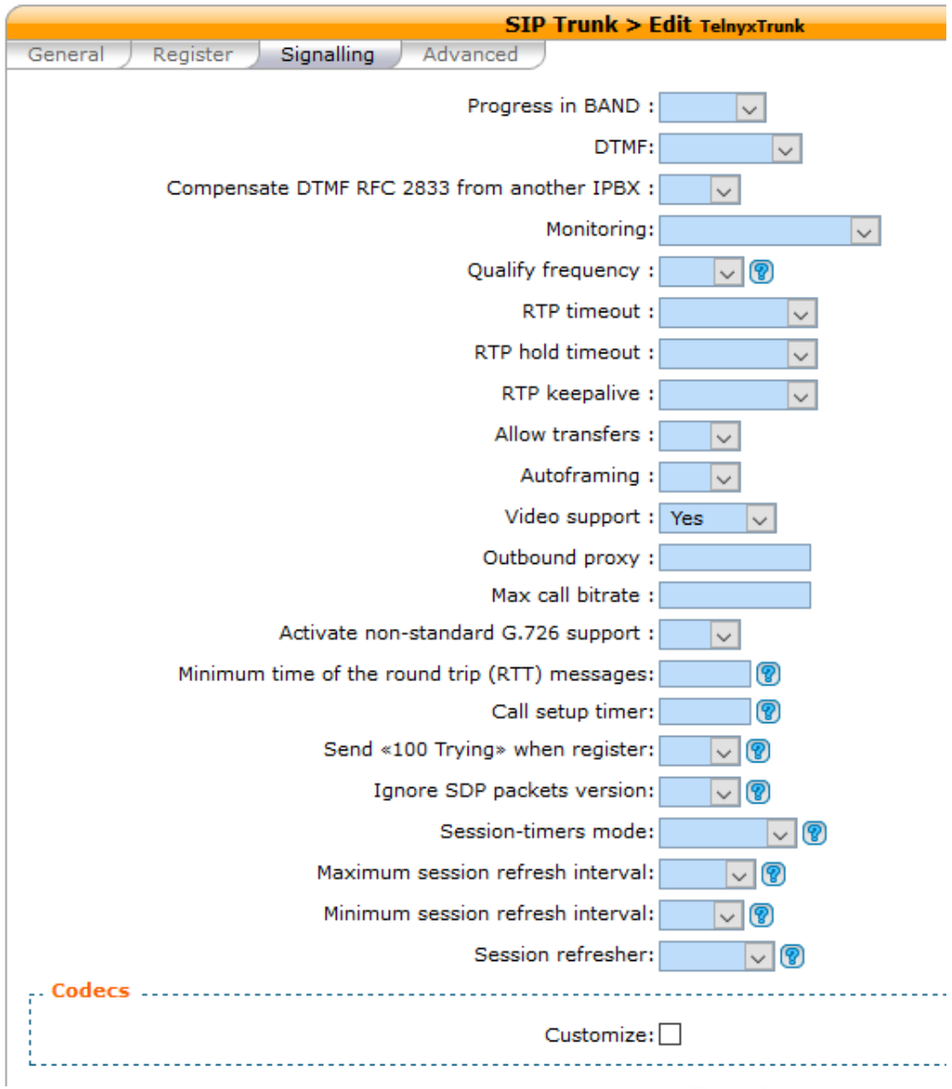


Go to CONFIGURATION:TRUNK MANAGEMENT:SIP PROTOCOL

Follow the settings in the screenshots to make sure your configuration will work with the firewall configuration. Pay attention to all settings.

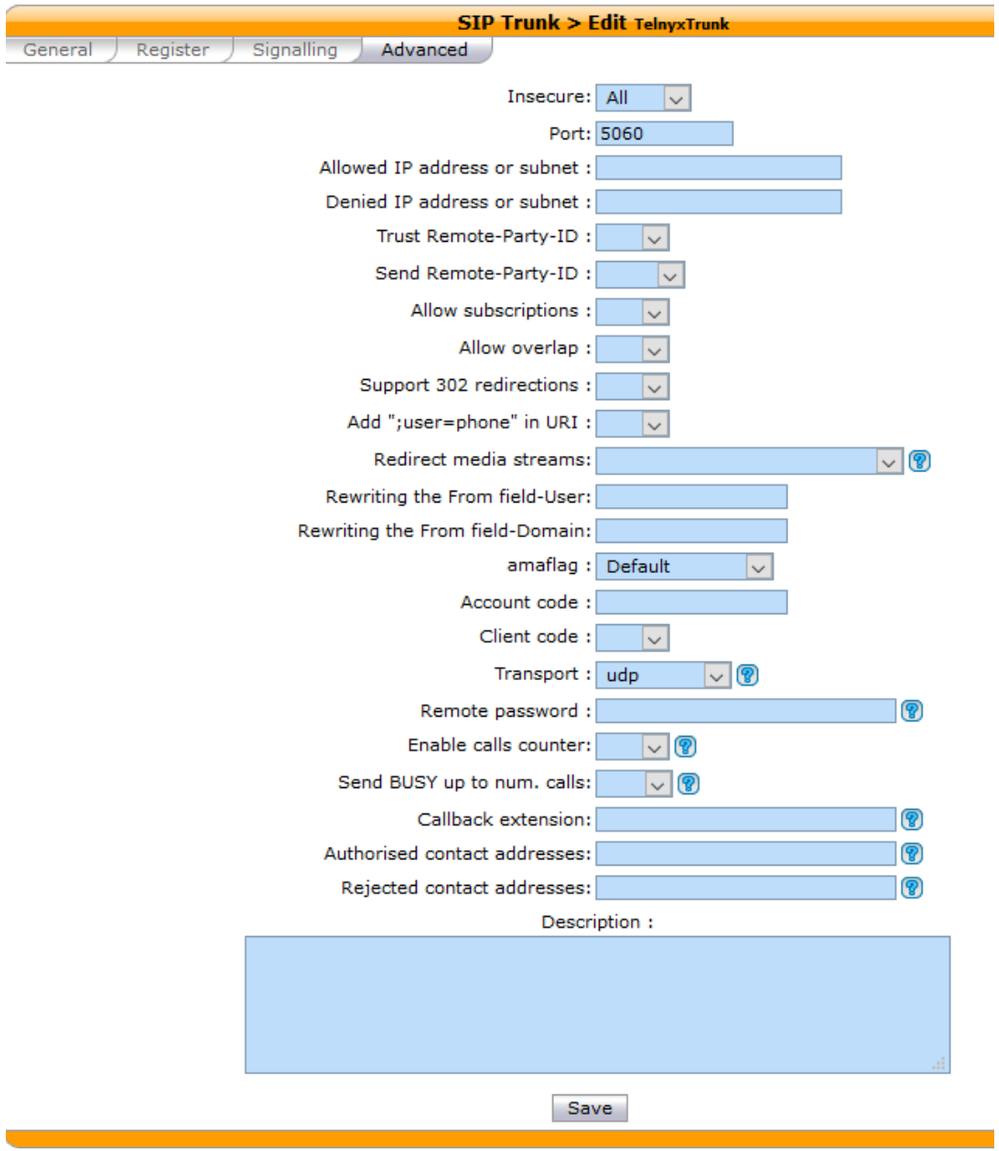






Go to CONFIGURATION:TRUNK MANAGEMENT:SIP PROTOCOL

Follow the settings in the screenshots to make sure your configuration will work with the firewall configuration. Pay attention to all settings.



Go to CONFIGURATION:CALL MANAGEMENT:OUTGOING CALLS

Put settings in to allow outgoing calls out the SIP trunk.