

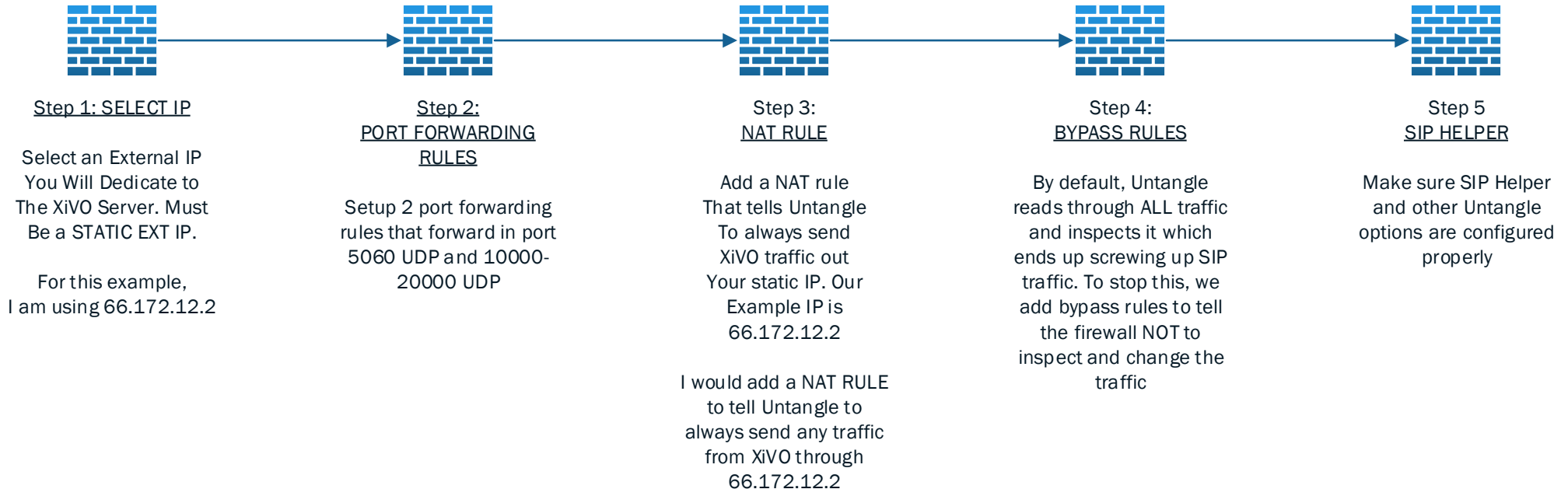
Configuring XiVO with Untangle Firewall

How to Successfully Firewall XiVO with Untangle



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





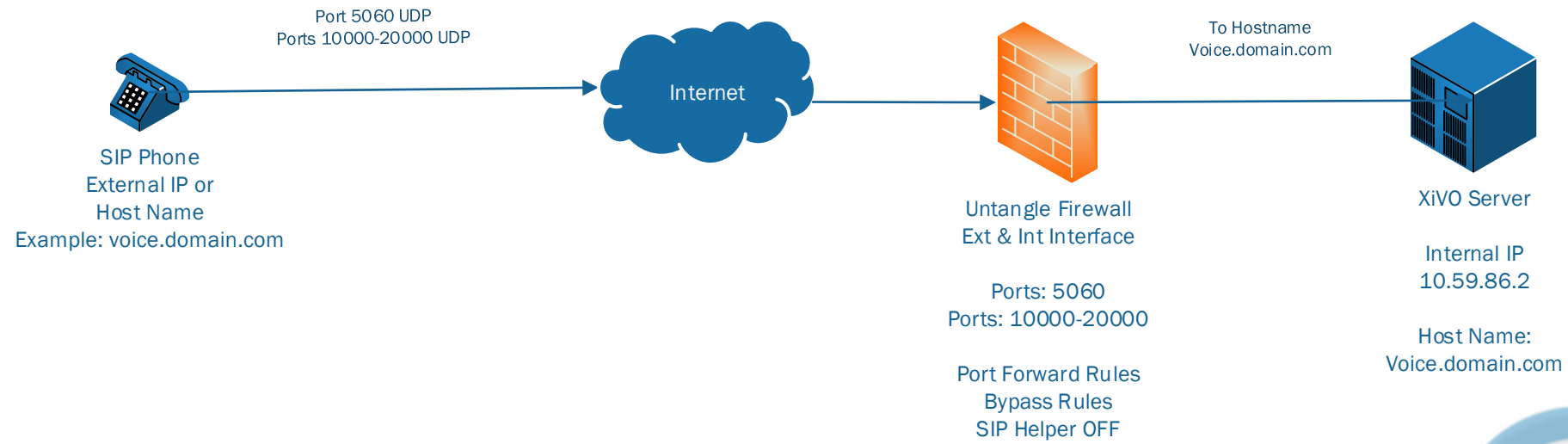
Untangle NAT RULES
[Untangle: CONFIG:NAT Rules: ADD](#)

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





Configuration > Network

Interfaces | Hostname | Services | Port Forward Rules | NAT Rules | Bypass Rules | Routes | DNS Server | DHCP Server | Advanced | Troubleshoot

Edit

Enable Port Forward Rule:

Description: VOIP 5060

If all of the following conditions are met:

Type	Value
Destination Address	is [External IP] Your External IP Here (Dedicated IP)
Destination Port	is 5060 Port 5060 Is Default Port for SIP Voice
Protocol	is <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TCP <input type="checkbox"/> ICMP <input type="checkbox"/> GRE <input type="checkbox"/> ESP <input type="checkbox"/> AH <input type="checkbox"/> SCTP

Forward to the following location:

New Destination: 10.59.86.2

New Port: (optional)

Put your Internal IP of your XiVO server here. Should be on the Internal Interface

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

UDP Only - You Don't Need TCP

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

Interfaces | Hostname | Services | Port Forward Rules | NAT Rules | Bypass Rules | Routes | DNS Server | DHCP Server | Advanced | Troubleshoot

Edit

Enable Port Forward Rule:

Description: SMS SIP 10000

If all of the following conditions are met:

Type	Value
Destination Address	is [External IP] Same Dedicated External IP
Destination Port	is 10000-20000 Open Ports 10000 through 20000
Protocol	is <input checked="" type="checkbox"/> UDP <input type="checkbox"/> TCP <input type="checkbox"/> ICMP <input type="checkbox"/> GRE <input type="checkbox"/> ESP <input type="checkbox"/> AH <input type="checkbox"/> SCTP

Forward to the following location:

New Destination: 10.59.86.2

New Port: (optional)

Put the internal IP of the XiVO server

UDP Only - No TCP

← Interfaces Hostname Services Port Forward Rules NAT Rules Bypass Rules Routes DNS Server DHCP Server Advanced Troubleshoot

Edit

Enable NAT Rule:

Description: SMS PBX 86

If all of the following conditions are met:

Type	Value
Source Address	10.59.86.2

Perform the following action(s):

NAT Type: Custom

New Source: 66.172.12.2 Example IP- Put Your External IP Here

Internal XiVO IP Here
Your XiVO should only have an internal IP sitting on the Untangle Internal Interface

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



The screenshot shows the 'Edit' configuration window for a Bypass Rule in Untangle. The 'Enable Bypass Rule' checkbox is checked. The 'Description' field contains 'SMS PBX 5060'. Under the 'If all of the following conditions are met:' section, a table lists one condition: 'Destination Port' is '5060'. The 'Perform the following action(s):' section shows the 'Action' set to 'Bypass'. A red box highlights the '5060' value in the condition table, and another red box highlights the 'Bypass' action dropdown.

Type	Value
Destination Port	5060

Set rule to bypass SIP traffic.

The screenshot shows the 'Edit' configuration window for a Bypass Rule in Untangle. The 'Enable Bypass Rule' checkbox is checked. The 'Description' field contains 'SMS PBX RTP'. Under the 'If all of the following conditions are met:' section, a table lists one condition: 'Destination Port' is '10000-20000'. The 'Perform the following action(s):' section shows the 'Action' set to 'Bypass'.

Type	Value
Destination Port	10000-20000

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



Advanced

Advanced settings require careful configuration. Misconfiguration can compromise the proper operation and security of your server.

Options QoS Filter Rules DNS & DHCP Network Cards

Enable SIP NAT Helper:

Send ICMP Redirects:

Enable STP (Spanning Tree) on Bridges:

DHCP Authoritative:

Block new sessions during network configuration:

Log bypassed sessions:

Log local outbound sessions:

Log local inbound sessions:

Log blocked sessions:

Session Viewer

Protocol	Bypassed	Policy	Client Interf...	Server Interf...	Hostname	Client (Pre-NAT)	Client Por...	Server (Post-NAT)	Server Po...	Username	Protochain (Application ...)
UDP	true		External	Internal		10.59.86.2	1025	10.59.86.2	5060		
UDP	true		Internal	External		10.59.86.2	123	10.59.86.2	123		
UDP	true		External	Internal		10.59.86.2	5060	10.59.86.2	5060		
UDP	true		External	Internal		10.59.86.2	1024	10.59.86.2	5060		
UDP	true		External	Internal		10.59.86.2	5060	10.59.86.2	5060		

All Sessions Refresh Auto Refresh Filter: 10.59.86.2 Case sensitive Clear Filters Clear Grouping Reset View

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.

IPBX
General settings
SIP Protocol
IAX Protocol
SCCP Protocol
Voicemails
Phonebook
Advanced
IPBX settings
Devices
Lines
Users
Groups
Voicemails
Conference rooms
Call management
Incoming calls
Outgoing calls
Call permissions
Call filters
Call pickups
Schedules
Calls Logs
Trunk management
SIP Protocol
IAX Protocol
Customized
IPBX services
Audio files
On-hold Music
Extensions
Paging
Phonebook
IPBX configuration
Backup Files
Configuration files
Contexts
LDAP filters
Control
Asterisk Log Files
Reload Asterisk
Restart Asterisk
Restart CTI server
Restart Dird server

SIP Protocol properties

General Network Security Signaling T38 Jitter Buffer Default Real time Internals

Auth. credentials

Replicate all these settings:

Port: 5060

UDP address: 0.0.0.0 Leave as 0.0.0.0

Allow TCP connections:

TCP address:

Automatic user creation: Persist

Accept unauthenticated calls:

Allow subscribe:

Allow overlap:

Match users with 'username' field:

Support 302 redirections:

Automatic domain:

Domain:

Use domain as realm:

Allow external domains:

Add ";user=phone" in the URI:

Realm: xivo

Reject invitations and recordings:

User-Agent: XiVO PBX

Audit did not conform to RFC new posts:

Recording context:

Force 'regexten' extension deactivation:

Caller ID: xivo

Rewriting the From field-Domain:

Debugging:

History save:

History recording:

Trigger 'peerstatus' event on auth failure:

TOS SIP:

TOS audio:

TOS video:

TOS text:

COS sip:

COS audio:

COS video:

COS text:

Save

SIP Protocol properties

General Network Security Signaling T38 Jitter Buffer Default Real time Internals

Auth. credentials

External IP address: 66.172.15.212

External domain:

Network transport protocols: udp

External TCP port:

External TLS port:

STUN address:

External domain refresh time: 10 seconds

Replace the IP or if it matches the external host LAN:

Deny dynamic ip address for static users and hosts:

Denied address/network:

Allowed address/network:

Outbound proxy:

Local network:

10.59.86.0/24

Save

SIP Protocol properties

General Network Security Signaling T38 Jitter Buffer Default Real time Internals

Auth. credentials

Allow TLS connections:

Listening address:

Server certificate:

CA certificate:

Don't verify server certificate:

TLS cipher:

Encryption:

Save

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:

Q580 reason:

enable SNOM AOC:

Subscribe network change event:

Max forwards:

Disallow methods:

Authenticate 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.723.1 (Audio)	+
G.729A (Audio)	-	GSM (Audio)	+
H.263 (Video)	-	G.711 A-law (Audio)	+
H.264 (Video)	-	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

SIP Protocol properties

General Network Security Signaling T38 Jitter Buffer Default Real time Internals

Auth. credentials

Username	Password type	Password	Realm	
No credentials				

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

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:



[Go to CONFIGURATION:NETWORK:Interfaces](#)

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

Interfaces > Edit

Interface:

Type: ?

Method:

Address:

Netmask:

Default gateway:

Description:



[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.

SIP Trunk > Edit TelnyxTrunk

General Register Signalling Advanced

Name:

Authentication username:

Password:

Caller ID:

Call limit:

Connection type:

IP Addressing type:

Context:

Language:

NAT:

SIP Trunk > Edit TelnyxTrunk

General Register Signalling Advanced

Register:

Transport:

Name:

Authentication username:

Password:

Remote server:

Port:

Use callback extension:

Contact:

Expiry:

SIP Trunk > Edit TelnyxTrunk

General Register Signalling Advanced

Progress in BAND:

DTMF:

Compensate DTMF RFC 2833 from another IPBX:

Monitoring:

Qualify frequency:

RTP timeout:

RTP hold timeout:

RTP keepalive:

Allow transfers:

Autoframing:

Video support:

Outbound proxy:

Max call bitrate:

Activate non-standard G.726 support:

Minimum time of the round trip (RTT) messages:

Call setup timer:

Send «100 Trying» when register:

Ignore SDP packets version:

Session-timers mode:

Maximum session refresh interval:

Minimum session refresh interval:

Session refresher:

Codecs

Customize:

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.

SIP Trunk > Edit TelnxTrunk

General Register Signalling **Advanced**

Insecure: All

Port: 5060

Allowed IP address or subnet :

Denied IP address or subnet :

Trust Remote-Party-ID :

Send Remote-Party-ID :

Allow subscriptions :

Allow overlap :

Support 302 redirections :

Add ";user=phone" in URI :

Redirect media streams: ?

Rewriting the From field-User:

Rewriting the From field-Domain:

amaflag: Default

Account code :

Client code :

Transport : udp ?

Remote password : ?

Enable calls counter: ?

Send BUSY up to num. calls: ?

Callback extension: ?

Authorised contact addresses: ?

Rejected contact addresses: ?

Description :

Save

Go to CONFIGURATION:CALL MANAGEMENT:OUTGOING CALLS

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

Outgoing calls > Edit telnx

General Exten Call permissions Schedules

Name: telnx

Context: SMS (to-extern)

Use ENUM:

Internal:

Preprocess subroutine:

Ring time before hangup: Unlimited

Trunks:

1 items selected	Remove all	<input type="text"/>	Add all
+ TelnxTrunk (SIP) -			

Description :

Save

Outgoing calls > Edit telnx

General Exten Call permissions Schedules

	Extern prefix	Prefix	Exten	Stripnum	Callerid	
1	<input type="text"/>	<input type="text"/>	1. <input type="text"/>	0	<input type="text"/>	?
2	<input type="text"/>	<input type="text"/>	0. <input type="text"/>	0	<input type="text"/>	?

Save