This page contains general information about port forwarding and disabling application layer gateways on particular routers.

Router Compatibility List

# Sonicwall

We have a document on setting up a Sonicwall here:

http://www.ipitomy.com/webrelease/Sonicwall/Sonicwall%20Quick%20Guide.pdf

We have seen that having IPS turned on with the check box for Prevent Low Priority Attacks checked can cause issues with some calls not going through. If you are having intermittent call failures try disabling this setting.

We have verified that enabling an inside--outside rule resolves the problems with dropped calls as it forces the Sonicwall to stick to port 5060. To configure this, create a NAT rule as follows:

Original Source: PBX Private IP
Translated Source: IP of the WAN interface (X1 IP for example)
Original Destination: Address Group for our SIP servers (52.5.220.123 or 54.200.236.200)
Translated Destination: Original
Original Service: Service Group including 5060 UDP and 10000-20000 UDP
Translated Service: Original
Inbound Interface: Any
Outbound Interface: WAN interface (X1 for example)

After that go to the Advanced tab and check the box for "http://wiki.ipitomy.comDisable Source Port Remap"http://wiki.ipitomy.com and click OK. The system will now talk to us from source port 5060.

### WARNING!

VoIP phones behind a firewall running SonicOS 6.2.7.1 cannot make outbounds calls, although inbound calls and phone registration are working fine. Occurs when the internal SIP device uses a port that is different from the source port (the port associated with the Via or Contact fields), and when the remote device sends packets to this port, the firewall is not forwarding them to the internal device.

# Mikrotik

This router has an ALG that can be disabled with the following command

- `/ip firewall service-port disable sip`

The info was found at the following two links Mikrotik Wiki Mikrotik Forum

# Fortigate

I found this online about solving issues with Fortigate routers and NO AUDIO with remote SIP:

In the command line of the fortigate type the following:

- `config system settings`
- `set sip-helper disable`
- `set sip-nat-trace disable`

Reboot the device

In the command line type the following:

- `config system session-helper`
- `show`

(now look for SIP, mostly it will be "http://wiki.ipitomy.com12"http://wiki.ipitomy.com)

- `delete 12`

Don't use any protection profiles on the firewall of the sip rules.

# Cisco Pix 506/501/515 and Cisco ASA

This is for Pix 506/501/515 but it should work with any Cisco Pix, and possibly other Cisco routers.

1. access-list 101 permit udp any host 64.238.XXX.XXX range 10000 20000
   (Note: Replace 64.238.XXX.XXX with your public IP assigned to be forwarded to the IPitomy PBX)
2. access-list 101 permit tcp any host 64.238.XXX.XXX range 10000 20000
   (Note: Replace 64.238.XXX.XXX with your public IP assigned to be forwarded to the IPitomy PBX)
3. static (inside,outside) 64.238.XXX.XX 172.16.2.129 netmask 255.255.255.255 0 0
   (Note: Replace 64.238.XXX.XXX with users public IP, replace the 172.16.2.129 with users private IP that is assigned to the IPitomy PBX)
4. no fixup protocol sip 5060
5. no fixup protocol sip udp 5060

# Adtran

From a recent interaction with an AdTran tech, it was shown to us there is a setting for "http://wiki.ipitomy.comproxy transparency"http://wiki.ipitomy.com that needs to be enabled in order for all of the SIP traffic to pass unhindered. This was when the Adtran was the routing device at the remote site, but likely would need to be enabled when the Adtran is at the PBX site. Its worth trying for sure.

# PepLink

Here is a document sent to a dealer from PepLink regarding configuration settings that may be required for Remote SIP to function properly:

Pdf:Peplink Config.pdf

# FIOS ActionTec

We have found the following article that outlines some possible configurations that are available on the Actiontec Modem/Router combo that FIOS is installing. This gives some options on ways to configure to optimize VoIP and SIP traffic passing to remote.

http://www.dslreports.com/faq/verizonfios/3.0_Networking#16077

# Comcast Modem

We have received some information from our dealers that if your site has a Comcast modem/router, you should request a SMC and not a Linksys, as the reports are that the SMC handles VoIP more consistently. Additionally, there may be issues with Comcast modem/routers ability to handle multiple concurrent NAT sessions, limiting the number of remote phones you can install at a remote site.

# Sophos

Some Sophos models have a hidden SIP module that is not in any way indicated, nor accessible, from the webgui. It must be disabled from the command line console. If left enabled, it attempts to override any rules you may have in place for sip/rtp traffic and can result in one-way audio, and other issues with calls successfully connecting.