

How to Disable SIP ALG on Popular Routers

SIP ALG (Application Layer Gateway) is a mechanism found in most routers that rewrites packets transmitted across the device. Certain protocols are processed by the application layer gateway (ALG) and rewritten to allow better flow through a firewall or when NAT (Network Address Translation) is employed. The SIP protocol is one of several protocols managed by this system.



One of the most common issues with VoIP solutions relates to audio transmission and presence of a firewall and/or NAT traversal being configured. In many cases, a properly configured system may still have audio issues when transmitting or receiving calls where only one party is heard during a call. Implementing the necessary changes to disable SIP ALG can oftentimes resolve these issues.

SIP ALG

What is SIP ALG and Why is it Bad?

The problem with SIP ALG is the fact that most times, packet rewriting causes undesirable operation. The intent of the technology was to assist the packet flow of SIP and other packets and help solve NAT related problems. In this case, the ALG's function is to perform a stateful packet level inspection (SPI) of traffic coming through it. SIP messages would then be re-written by SIP ALG to allow the correct communication of signaling and voice traffic between endpoints and effective NAT traversal. The frequent result in lower end routers is however a hindrance for data transmission due to poor implementations of ALG that break SIP. Most commonly, the issues many experience relate to one-way or no audio, depending on who initiates the call.

In most cases, it is recommended that SIP ALG, SPI and SIP transformations are disabled.

Navigating SIP ALG

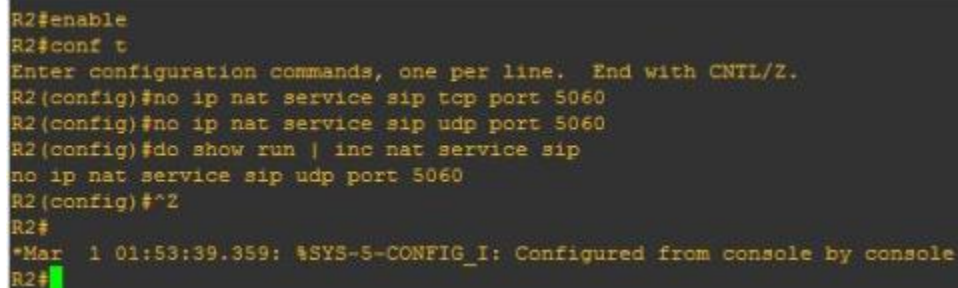
With most setups, it is best to disable this feature as this service usually does more harm than good. The following section will help to assist most with disabling this feature on their router. The first few sections will cover the basis of disabling SIP ALG and SPI for higher-class enterprise devices while the lower sections relate to common devices used in small offices or homes.

Cisco Router

If running a business class Cisco router, you can initiate a terminal session with an application like PuTTY

or directly accessing the console. Enable privileged EXEC mode and issue the following commands where 'ciscohost' is the name of your router (see Figure 1 too):

```
ciscohost# conf t
ciscohost(config)# no ip nat service sip tcp port 5060
ciscohost(config)# no ip nat service sip udp port 5060
ciscohost(config)# do show run | inc nat service sip
```



```
R2#enable
R2#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#no ip nat service sip tcp port 5060
R2(config)#no ip nat service sip udp port 5060
R2(config)#do show run | inc nat service sip
no ip nat service sip udp port 5060
R2(config)#^Z
R2#
*Mar  1 01:53:39.359: %SYS-5-CONFIG_I: Configured from console by console
R2#
```

Figure 1: Disabling SIP Inspection on a

Cisco Router

If it worked, the next line displayed after the **"do show"** command will read "no ip nat service sip tcp port 5060" and **"no ip nat service sip udp port 5060"**. After this message appears, press [CNTRL] + [z] to end the configuration session.

In general though, Cisco routers have a high quality SIP ALG implementation that should work well and not cause any issues.

Cisco ASA (Adaptive Security Appliance)

Unless you maintain the network at your business, you probably will not have access to the ASA. Making changes to this device is not recommended unless you know what you are doing.

Access the console and enable elevated privileges. Enter the following commands to turn off SIP inspection at a global level.

```
ciscofirewall# enable
Password:
ciscofirewall# conf t
ciscofirewall# policy-map global_policy
ciscofirewall# no inspect sip
ciscofirewall# show run | inc policy-map global-policy | inspect sip
ciscofirewall# end
```

For most Cisco ASA models, this will effectively disable SIP inspection for the entire system. If keen to learn and experiment with Cisco solutions, I suggest using the emulator furnished by **GNS3**. However, such configuration techniques are far beyond the scope of this article.

Cisco ASDM (Adaptive Security Device Manager)

The ASDM client for Cisco devices provides a visual interface for ASA systems, both virtual and physical. If the ASA at your business is manageable by this client, the following techniques should prove to be an

easier way for accomplishing the same task compared to the command line techniques described in the previous section.

* Navigate to the interface while on the same LAN by typing the IP address of the machine in a browser window. If the ADSM client resides on your machine and the system is ADSM capable, a prompt should appear that requests permission to launch the application. * Each system and version are slightly different. Essentially, you as the user will need to find the Configuration area, select the Firewall option and go into the Service Policy Rules area. (Note: systems may use slightly different verbiage for each section though the methodology described above should be exactly what is needed for most systems.) * Find something resembling a “policy rule” area. Select an item where inspection_ precedes the object/item definition and edit the policy (usually by right-clicking though some interfaces will require selecting the item with a left-click and selecting the Edit item from the bar above). * A tab in the next menu should read something similar to Rules Actions. Find a tab or item where the work protocol is used and inspect the items in this list. Locate the SIP item and uncheck the item. Save the settings after completion.

Note that this will apply a global setting to your entire device. For port specific settings, navigate to the settings for each port and alter if necessary.

SonicWall

Like Cisco, slightly different interfaces are common, relative to the version and model of the system. Generally speaking, these devices are fairly simple to configure with administrative privileges handy. While on the LAN where the device resides, type in the IP address or host name (if DNS is configured) to access the configuration area.

From the main menu, find the “VoIP” option that usually appears on the left menu. While in the menu, uncheck the box for SIP - it often appears as “SIP Transformations” and then select the option to “Enable Consistent NAT”. Accept the settings and reboot if prompted. Figure 2 shows an example of the SonicWall user interface on the page where these settings exist.

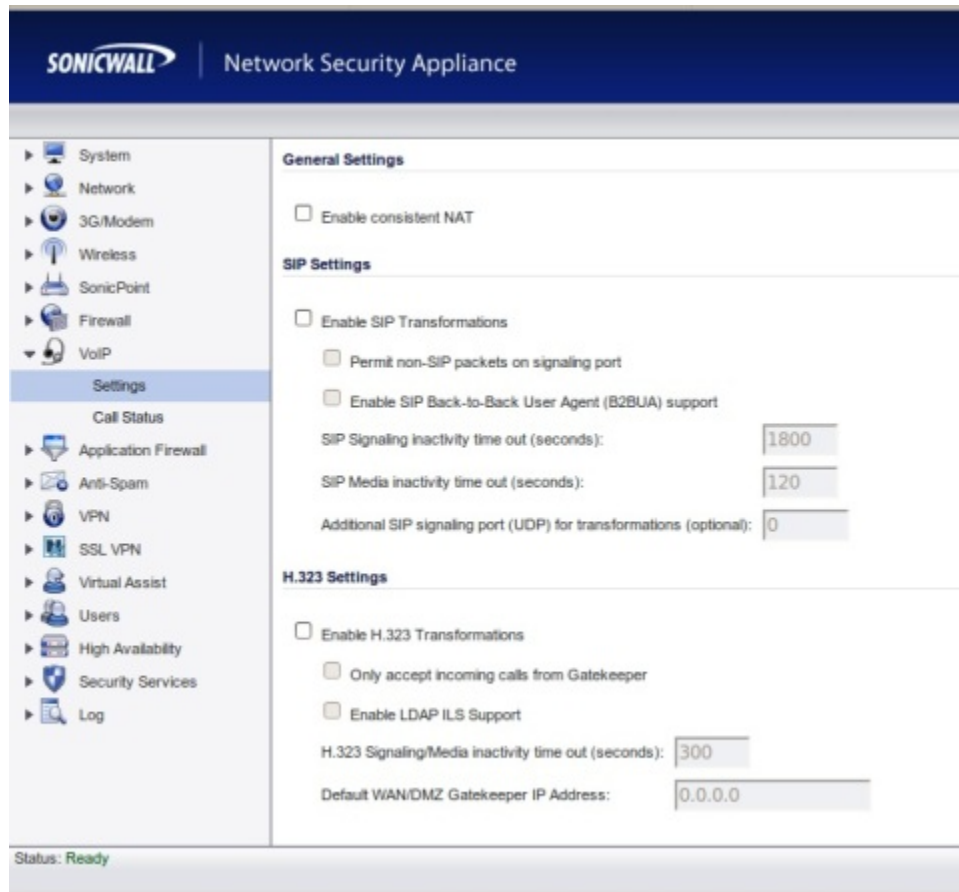


Figure 2: Disabling SIP ALG on a SonicWall

Router

Understand that although this method seems quite generalized, it is the basis for disabling SIP intervention on most SonicWall systems.

Netgear

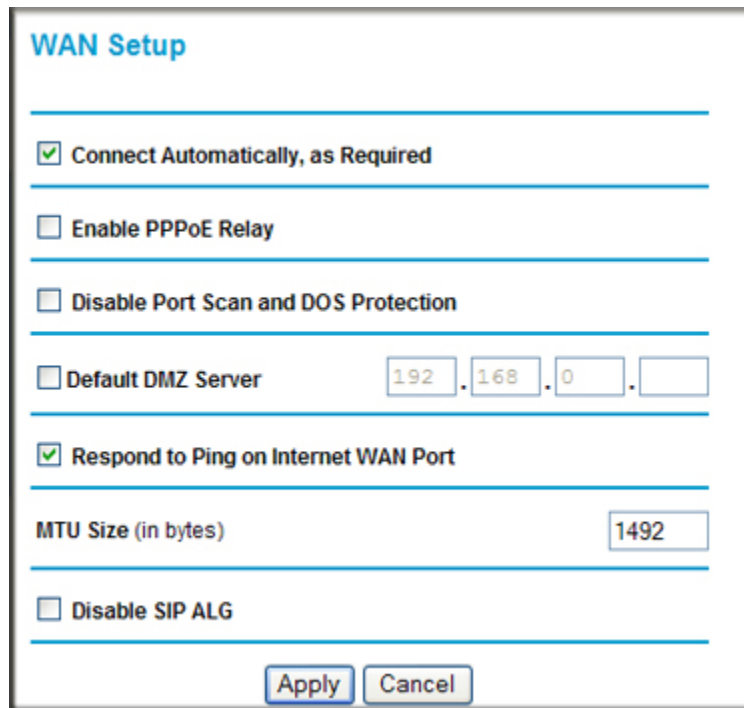
Netgear has several different interfaces. As this brand is one of the most popular for home and small business networking, variation in interfaces is common due to the large number of devices made by the company. However, the following example should provide a good reference for the more common models and show you how to disable SIP ALG on your Netgear router.

While connected to the LAN, open a browser and enter the router's IP address.

Enter the authentication credentials - defaults are usually 'admin' for the username and "password" for the password.

Find the WAN setup option and locate the item where SIP is mentioned (usually, this falls under the Advanced tab).

Most models have a check-box reading something similar to "Disable SIP ALG" in figure 3 below. Check the box, apply the settings and reboot if prompted.



WAN Setup

☒ Connect Automatically, as Required

☐ Enable PPPoE Relay

☐ Disable Port Scan and DOS Protection

☐ Default DMZ Server . . .

☒ Respond to Ping on Internet WAN Port

MTU Size (in bytes)

☐ Disable SIP ALG

Figure 3: Disabling SIP ALG on a SonicWall

Router

D-Link

Like Netgear, D-Link has a variety of different interfaces but the methodology for disabling this setting is very similar for most models. Many models are equipped with a powerful set of firewall tools so several steps must be completed to ensure SIP traffic passes beyond the device.

Open a browser and enter the router's IP address in the address bar. Go to **"Firewall Settings"** under the **"Advanced"** item.

Uncheck the box to disable SPI - usually, directly below this item are options for **"NAT Endpoint Filtering"** that must be changed to **"Endpoint Independent"** for both TCP and UDP.

Next, find the **"Application Level Gateway (ALG) Configuration"** area and uncheck the box for SIP.

Save these settings and reboot the device if requested. Figure 4 below shows additional details on how to configure this setting:

DIR-655 // **SETUP** **ADVANCED** **TOOLS** **STATUS**

VIRTUAL SERVER
PORT FORWARDING
APPLICATION RULES
QOS ENGINE
NETWORK FILTER
ACCESS CONTROL
WEBSITE FILTER
DISQUID FILTER
FIREWALL SETTINGS
ROUTING
ADVANCED WIRELESS
WDSH
WI-FI PROTECTED SETUP
ADVANCED NETWORK
SECURESPOT
GUEST ZONE

FIREWALL SETTINGS

The Firewall Settings allow you to set a single computer on your network outside of the router.

Save Settings Don't Save Settings

FIREWALL SETTINGS

Enable SPI : ☐

NAT ENDPOINT FILTERING

UDP Endpoint Filtering: ☐ Endpoint Independent ☒ Address Restricted ☐ Port And Address Restricted

TCP Endpoint Filtering: ☐ Endpoint Independent ☐ Address Restricted ☒ Port And Address Restricted

ANTI-SPOOF CHECKING

Enable anti-spoof checking: ☐

DMZ HOST

The DMZ (Demilitarized Zone) option lets you set a single computer on your network outside of the router. If you have a computer that cannot run Internet applications successfully from behind the router, then you can place the computer into the DMZ for unrestricted Internet access.

Note: Putting a computer in the DMZ may expose that computer to a variety of security risks. Use of this option is only recommended as a last resort.

Enable DMZ: ☐

DMZ IP Address : 0.0.0.0 << Computer Name

APPLICATION LEVEL GATEWAY (ALG) CONFIGURATION

PPTP : ☒
 IPsec (VPN) : ☒
 RTSP : ☒
 SIP : ☐

Figure 4: Disabling SIP ALG on a D-Link

Router

AT&T (2WIRE)

At the time this article was written, most AT&T services - whether DSL or UVERSE - are packaged with a 2WIRE device. Fortunately, the company allows disabling the service with minimal headache for most models and services. Yet, some models do not have this feature making this process cumbersome.

Type in the device IP address of <http://192.168.1.254> in any browser address bar. Default username is "admin" and the password can be found on the bottom on the 2wire device.

Go to the "Firewall" menu and then select the option for "Applications, Pinholes and DMZ". Select your phone adapter from the the list of IP addresses and then the radio button to "Allow all applications (DMZplus mode)". Save the settings and you have now put your adapter in the DMZ plus zone.

SIP ALG now needs to be disabled via the 'Management and Diagnostic Console' that can be accessed by entering <http://192.168.1.254/mdc> (note that not all models of 2wire modems can access this menu and edit the settings).

If you can access this console, click on the "Configure Services" found under the "Advanced" heading.

A setting notated as "SIP Application Layer Gateway" should be unchecked - hit the [SUBMIT] item and follow any additional prompts. See figure 5 below for a screen shot:

Figure 5: Disabling SIP ALG on a AT&T 2Wire Modem

Some have stated that it is not possible to turn off this setting. Newer firmware deployments on current models (as of April 2015, when this article was originally written) may not allow disabling this option. Contacting customer service to remote into your device will be the only way to turn off this setting.
Comcast | Xfinity

At the time this article was written (April 2015), there is no possible way to disable SIP ALG on a Comcast router by yourself. Worse yet, the company will not disable this feature for most customers.

Since both residential and business customers do not have an option to disable this setting from the router configuration menu, using VoIP means one of the following options will be necessary:

Buying the Comcast / Xfinity phone service.
Hope your service transposes appropriately with SIP ALG.
Connect another router to you gateway and put it in bridge mode.
Purchase your own gateway compatible with Comcast/Xfinity.

The company locks down the devices such that the only voice service allowed is Comcast/Xfinity. The recommended solution involves purchasing a compatible modem for the service where greater control is possible. At this point, contact your VoIP vendor - many have unique firmware settings to push to the device as well as instructions for applying settings for a functional service. Final Thoughts

Most agree that SIP ALG is the ultimate bane for VoIP services. Sadly, this technology that is supposed to help such transmissions proves to be a hindrance for virtually every product and service in existence. Though many companies have a workaround, some lack a solid solution.

We are very interested in hearing your unique problems and resolutions involving this mechanism and if you would like us to investigate other routers. Please, take a moment to comment or ask a question - we would like to help as many VoIP consumers as possible!

From:
<https://wiki.ring-u.com/wiki/> - **support wiki**

Permanent link:
<https://wiki.ring-u.com/wiki/doku.php?id=disablesipalg&rev=1654109945>

Last update: **2022/06/01 18:59**

