ALG

About

An ALG (Application Layer Gateway) is a security component, commonly found in a router or firewall device, that is supposed to enhance the ability for certain protocols to traverse NAT. A more complete discussion can be found here and here.

Discussion

While ostensibly a SIP ALG is designed to enhance SIP and make the notoriously problematic NAT traversal issues easier to deal with, the simple fact of the matter is that most SIP ALG's are horribly broken. Brian K West has described them as "evil" - which is not really an understatement if you've ever been burned by one. Most routers that have SIP ALG's come with them enabled by default, which means that it's up to the user or admin to dig into the configuration to disable them. The following sections contain instructions and links to more information about various devices that have SIP ALG's and how to disable them. Also, be mindful of the fact that some manufacturers have created devices whose SIP ALG's cannot be disabled. AVOID THEM LIKE THE PLAGUE. (I'm talking to you, Netgear.)

The simple solution to this is to use encrypted communications. Since TLS packets cannot be read nor modified by the router, SIP ALGs will never be able to mangle encrypted calls. yet another reason go encrypted.

TLS

For encrypted calls you will **always** need to support NAT traversal on the SIP client itself.

Even if you're only making unencrypted calls using SIP ALG it is far better to get your phone or edge router correctly to handle that NAT on its own for all calls from the very start. That way you won't experience problems if you switch to TLS encrypted calls; or need to make configuration changes when switching between unencrypted and encrypted calls.

Disabling ALG

Following are some specific instructions on how to disable SIP ALG on various consumer– and business–grade routers. Please add any devices that you know of in the comment section at the bottom of the page. Also, if you know of some devices that cannot disable their built-in SIP ALG please list or link to them there.

Linux netfilter iptables

iptables has two loadable modules (nf_conntrack_sip and nf_nat_sip) for processing SIP packets. nf_nat_sip contains all the SIP ALG functionality. To unload the ALG use the following command:

```
modprobe -r nf_nat_sip
```

The nf_conntrack_sip module tracks open connections, e.g. for automatically opening RTP ports; it does not perform ALG and does not modify the packets, and so can safely be left loaded.

This may also work on Linux-based routers without an option if you gain command line access (e.g. Netgear), although it may not persist on reboot.

If you use a firewall product that acts as a front-end to iptables, you may need to reconfigure that product to prevent it loading nf_nat_sip.

2Wire 3800

I have UVerse from AT&T and my VoIP calls were horrible until I realized that I had this device. I found the instructions found at the Verizon on-line support site to be quite simple and accurate. The Verizon site has actual screen shots. For those of you who don't need a picture, these are the steps:

1. Open browser, type the router's IP address followed by **/mdc**
   e.g. http://192.168.1.254/mdc
2. Enter the password and click submit or press Enter.

3. On the left navigation bar under "Advanced", click on "Configure Services" link
4. Clear the "Enable" checkbox under SIP Application Layer Gateway
5. Click submit
6. Enjoy unfettered VoIP calls!

Thompson/Alcatel Speedtouch 510/530

This router can cause Authentication to fail with UDP. There is no web option to disable ALG, so you have to do the following:

1. telnet to the router (normally 10.0.0.138)
2. Unbind the SIP protocol and reboot the modem by entering the following commands:
    a. nat unbind application=SIP port=5060
    b. config save
    c. system reboot

Dlink DIR 625/628/655

Disable SIP ALG as follows:

under "Advanced"->"Firewall Settings"->"Application Level Gateway (ALG) Configuration", clear the "SIP" checkbox.

D-Link EBR-2310

1. Navigate to the routers web interface, usually at http://192.168.0.1
2. The Default Login Credentials are username=admin password=<blank>
3. Select "Advanced"
4. Select "Firewall Settings" from the left navigation pane.
5. Clear the "Enable SPI" checkbox so that SPI is disabled
6. Clear the "SIP" checkbox in the Application Level Gateway Section so that SIP ALG is disabled

SonicWall with SonicOS Enhanced

These routers will function as expected for a period of time, then for no apparent reason cause certain SIP endpoints to fail to authenticate. Using TCP over SIP has resolved the issue in my cases. To disable SIP ALG from the web interface:

1. Open web administration interface
2. Select VoIP from the left menu
3. Clear the "Enable SIP Transformations" checkbox
4. Click Accept

Netgear DG834G

1. Navigate to the routers web interface. Usually at http://192.168.0.1
2. The Default Login Credentials are username=admin password=password
3. Select "WAN Setup" from the left navigation menu.
4. Check the "Disable Port Scan and DOS Protection" checkbox
5. Check the "Disable SIP ALG" checkbox

Netgear WNDR3300

1. Navigate to the router's web interface, usually at http://192.168.1.1
2. The Default Login Credentials are username=admin password=password
3. Select "WAN Setup"
4. Check the "Disable SPI" checkbox so that SPI is disabled
5. Check the "Disable SIP ALG" checkbox so that SIP ALG is disabled

Other Options

Some have reported that using SIP over TCP can avoid SIP ALG issues. FS user Moc reports that SIP over TCP has helped him deal with multiple issues with SonicWall routers. Give it a try before you throw money down on a new piece of hardware.

Keep in mind, though, that this will only work as long as vendor products are only inspecting for SIP over UDP. Sooner or later they may extend that to TCP as well. After all, there's nothing stopping them.

The only "sure fire" and universal way to defeat SIP ALGs is to use TLS. Not only does it usually run over a different port (5061) it appears just like another TLS data stream and because it's encrypted the router has no chance of modifying the payload of the packets. When in doubt, use TLS. If you're planning on doing a large SIP deployment and your devices support it, use TLS. You'll save yourself a lot of time and hassle.