

# **SIP ALG**

**O QUE É E COMO DESABILITAR SIP ALG**

**net2phone**

An IDT Company

## O que é o SIP ALG?

SIP ALG significa Application Layer Gateway e é comum em muitos roteadores comerciais. Seu objetivo é evitar alguns dos problemas causados pelos firewalls do roteador, inspecionando o tráfego de VoIP (pacotes) e, se necessário, modificando-o.

## Muitos roteadores têm o SIP ALG ativado por padrão.

Existem várias soluções para clientes SIP por trás do NAT, algumas no lado do cliente (STUN, TURN, ICE), outras no lado do servidor (Proxy RTP como RtpProxy, MediaProxy).

De um modo geral, o ALG funciona normalmente no roteador ou gateway da LAN do lado do cliente. Em alguns cenários, outras soluções do lado do cliente não são válidas, por exemplo, STUN com roteador NAT simétrico. Se o proxy SIP não fornecer uma solução NAT do lado do servidor, uma solução ALG poderá ter um lugar.

Um ALG entende o protocolo usado pelos aplicativos específicos que ele suporta (neste caso, SIP) e faz uma inspeção de pacotes de protocolo do tráfego através dele. Um roteador NAT com um SIP ALG embutido pode reescrever informações nas mensagens SIP (cabeçalhos SIP e corpo SDP), possibilitando o tráfego de sinalização e áudio entre o cliente atrás do NAT e o endpoint SIP.

## Como isso pode afetar o VoIP?

Embora o SIP ALG tenha como objetivo ajudar os usuários que possuem telefones em endereços IP privados (Classe C 192.168.X.X), em muitos casos, ele é implementado de maneira inadequada e causa mais problemas do que resolve. SIP ALG modifica pacotes SIP de maneiras inesperadas, corrompendo-os e tornando-os ilegíveis. Isso pode gerar um comportamento inesperado, como telefones não registrados e falha de chamadas recebidas.

Portanto, se você estiver enfrentando problemas, recomendamos que verifique as configurações do roteador e desative o SIP ALG, caso esteja ativado.

- **Falta de chamadas recebidas:** quando um UA é ativado, ele envia uma solicitação de REGISTRO ao proxy para ser localizável e receber todas as chamadas recebidas. Este REGISTRO é modificado pelo recurso ALG (caso contrário, o usuário não seria acessível pelo proxy, pois indicava um IP privado no cabeçalho "Contato" do REGISTRO). Os roteadores comuns apenas mantêm a "conexão" UDP aberta por um tempo (30 a 60 segundos); após esse período, o encaminhamento da porta termina e os pacotes recebidos são descartados pelo roteador. Muitos proxies SIP mantêm o UDP keepalive enviando mensagens OPTIONS ou NOTIFY para o UA, mas apenas o fazem quando o UA foi detectado como NAT durante o registro. Um roteador SIP ALG reescreve a solicitação REGISTER no proxy não detecta o NAT e não mantém o keepalive (portanto, as chamadas recebidas não serão possíveis).
- **Interrompendo a sinalização SIP:** Muitos dos roteadores comuns reais com SIP ALG embutido modificam os cabeçalhos SIP e o corpo do SDP incorretamente, interrompendo o SIP e impossibilitando a comunicação. Alguns deles fazem uma substituição completa pesquisando um endereço privado em todos os cabeçalhos e corpo do SIP e substituindo-os pelo endereço público mapeado do roteador (por exemplo, substituindo o endereço privado se ele aparecer no cabeçalho "Call-ID", o que não faz sentido em absoluto). Muitos roteadores SIP ALG corrompem a mensagem SIP ao gravá-la (ou seja, ponto e vírgula ausente ";" nos parâmetros do cabeçalho). Escrever valores de porta incorretos maiores que 65536 também é comum em muitos desses roteadores.

- Não permite soluções do lado do servidor: mesmo que você não precise de uma solução NAT do lado do cliente (seu proxy SIP fornece uma solução NAT do servidor), se o seu roteador tiver o SIP ALG ativado que interrompa a sinalização SIP, ele fará a comunicação com o seu proxy impossível.

## **Desativei o SIP ALG, mas ainda estou com problemas ...**

Se você ainda estiver tendo problemas após desativar o SIP ALG, verifique sua configuração de firewall.

## **Não consigo desativar o SIP-ALG? Como circunavegar qualquer implementação quebrada de fornecedores de rede do SIP ALG**

- Habilite o TLS nos terminais SIP, o VoiceHost suporta TLS, que mascara a sinalização SIP dos olhos curiosos da funcionalidade ALG.
- Habilite o IPv6 nos terminais SIP. Praticamente essa não é uma opção realista para usuários que precisam de mobilidade, mas para locais estáticos, isso remove o requisito (deve ser suportado pelo seu ISP). A maioria dos provedores de Internet não suporta totalmente IPv6 puro.
- Troque seu roteador em um último recursos se tudo mais falhar.

## Como desativo o SIP ALG?

A maioria dos roteadores domésticos / residenciais possui uma interface da web. Normalmente, é por meio do endereço de IP 192.168.1.1, mas você apenas verifica seu gateway padrão digitando ipconfig no prompt de comando do Windows ou ifconfig nos sistemas Linux a partir de qualquer dispositivo conectado na mesma LAN.

Se o seu roteador não tiver uma interface da web, você provavelmente precisará de um cliente Telnet para fazer login.

Se você não possui um cliente de telnet instalado, recomendamos o Smartty ([smartty.sysprogs.com](http://smartty.sysprogs.com))

Conecte-se no telnet ao endereço IPv4 do seu gateway e pressione Enter novamente..

|                                       |   |
|---------------------------------------|---|
| <p><b>Asus Routers</b></p>            | <p>Disable the option SIP Passthrough under Advanced Settings / WAN -&gt; NAT Passthrough.<br/>If your router doesn't have this option SIP ALG may be disabled via Telnet.</p> <pre><i>nvr</i>am get nf_sip <i>(It should return a "1")</i></pre> <pre><i>nvr</i>am set nf_sip=0 <i>nvr</i>am commit Reboot</pre> |
| <p><b>AVM<br/>Fritz!Box</b></p>       | <p>SIP ALG cannot be disabled. (See above on how to get around this)</p>  |
| <p><b>Barracuda<br/>Firewalls</b></p> | <p>Go to Firewall &gt; Firewall Rules &gt; Custom FirewallAccess Rules<br/>Click the "Disabled" check box next to any rules named LAN-2-INTERNET-SIP and INTERNET-2-LAN-SIP<br/>This disables SIP ALG.</p>  |
| <p><b>Billion</b></p>                 | <p>Navigate to the web interface<br/>-&gt; Select Configuration<br/>-&gt; Select NAT<br/>-&gt; Select ALG<br/>-&gt; Disable SIP ALG</p>   |
| <p><b>BT<br/>(Homehubs)</b></p>       | <p>SIP ALG cannot be disabled in the settings of BT HomeHubs but can be disabled with BT Business Hub versions 3 and higher.</p>  |
| <p><b>D-Link</b></p>                  | <p>In 'Advanced' settings --&gt; 'Application Level Gateway (ALG) Configuration' un-tick the 'SIP' option.</p>  |

|                        |  |
|------------------------|--|
| <p><b>DD-WRT</b></p>   | <p><b>No ALG function available - Consider using a public STUN server</b></p>  |
| <p><b>DrayTek</b></p>  | <p>DrayTek Vigor 2760 devices, the option can be found in the regular interface at Network -&gt; NAT -&gt; ALG.</p> <p>If your device does not have a web interface then you'll need a telnet client.</p> <p>You will be prompted to provide a username and/or password. These are the same credentials used to access the router's web interface.</p> <p>Afterwards, type in these commands:</p> <pre>sys sip_alg 0 sys commit</pre> <p>On Draytek Vigor2750 and Vigor2130 please use these commands instead:</p> <pre>kmodule_ctl nf_nat_sip disable kmodule_ctl nf_contrack_sip disable</pre> |
| <p><b>EE</b></p>       | <p>Huawei E5330</p> <p>Navigate to the web interface</p> <p>Click Settings.</p> <p>Enter the required username and password, then click Log In.</p> <p>Note: The default username and password is admin.</p> <p>Click the Security dropdown.</p> <p>Click SIP ALG Settings.</p> <p>Untick the Enable SIP ALG box.</p> <p>Click Apply.</p>  |
| <p><b>Fortinet</b></p> | <p>Fortigate:</p> <p>Disabling the SIP ALG in a VoIP profile</p> <p>SIP is enabled by default in a VoIP profile. If you are just using the VoIP profile for SCCP you can use the following command to disable SIP in the VoIP profile.</p> <pre>config voip profile edit VoIP_Pro_2 config sip set status disable end</pre>  |

|                                  |   |
|----------------------------------|---|
| <p><b>Huawei</b></p>             | <p>The SIP ALG setting is usually found in the Security menu.</p> <ol style="list-style-type: none"> <li>1. Vodafone / Huawei (HHG2500)</li> <li>2. TalkTalk / Huawei (HG633)</li> <li>3. EE / Huawei (E5330)</li> </ol>  |
| <p><b>Juniper</b></p>            | <p>Type the following into the CLI</p> <p>To check if currently enabled or disabled run show security alg status   match sip</p> <p>To disable run:</p> <pre>configure set security alg sip disable commit</pre>  |
| <p><b>Linksys:</b></p>           | <p>Check for a SIP ALG option in the Administration tab under 'Advanced'.</p> <p>You should also disable the SPI Firewall option.</p>   |
| <p><b>Mikrotik</b></p>           | <p><b>Disable SIP Helper.</b></p>   |
| <p><b>Netgear</b></p>            | <p>Look for a 'SIP ALG' checkbox in 'WAN' settings.</p> <p>Under 'NAT Filtering' uncheck the option 'SIP ALG'</p> <p>Port Scan and DoS Protection should also be disabled.</p> <p>Disable STUN in VoIP phone's settings.</p>  |
| <p><b>openwrt</b></p>            | <p><b>No ALG feature - Consider using a public STUN server</b></p>  |
| <p><b>PfSense</b></p>            | <p><a href="https://www.voicehost.co.uk/help/pfsense-voip-configuration">https://www.voicehost.co.uk/help/pfsense-voip-configuration</a></p>  |
| <p><b>SonicWALL Firewall</b></p> | <p>Under the VoIP tab, the option 'Enable Consistent NAT' should be enabled and 'Enable SIP Transformations' unchecked.</p> <p>Detailed instructions can be found here: <a href="https://www.voicehost.co.uk/help/sonicwall-configuration">https://www.voicehost.co.uk/help/sonicwall-configuration</a></p> |
| <p><b>Speedtouch</b></p>         | <p>To disable SIP ALG you need to telnet into your Speedtouch router and type the following:</p> <pre>-&gt; connection unbind application=SIP port=5060 -&gt; saveall</pre>   |

|  |  |
|--|--|
| <p><b>TalkTalk</b></p>   | <p>2017/18 See Huawei (HG633)</p> <ol style="list-style-type: none"> <li>1. Navigate to the web interface</li> <li>2. Select 'Port Forwarding' from the menu</li> <li>3. Uncheck SIP-ALG from the ALG section at the bottom of the page.</li> </ol>  |
| <p><b>Technicolor / Thompson</b></p> <p><b>TG588 TG589</b></p> <p><b>TG582</b></p> | <p>Open Command Prompt - "Start" → "Run" → type "cmd" and press "Enter".<br/>         In Command Prompt, type "telnet 192.168.1.254" and press enter. 192.168.1.254 is the default IP address of the router. If you are running on Windows 7/8/8.1/10, you might need to install the telnet client from "Control Panel" → "Programs and Features" → "Turn Windows features on and off".<br/>         The default username is "Administrator", and there is no default password, leave blank.<br/>         Type "connection unbind application=SIP port=5060" and press "Enter".<br/>         Type "saveall " and press "Enter".<br/>         Type "exit" and press "Enter" to exit the telnet session.</p> |
| <p><b>Tomato</b></p>   | <p>Depending on the version of Tomato, SIP ALG can be found under Advanced then Conntrack/Netfilter in the Tracking/NAT Helpers section. If you find SIP checked then SIP ALG is enabled. Uncheck it to disable it.</p>  |
| <p><b>TP-Link</b></p>  | <p>Navigate to your routers web interface.<br/>         The default username is admin and the default password is admin.<br/>         On the left, click on Advanced Setup and then click on NAT and then click on ALG.<br/>         Uncheck the box by SIP Enabled. (Some TP firmware shows this as SIP Transformations which is the same thing).<br/>         Click Save/Apply.</p>  |
| <p><b>UBEE Gateways</b></p>  | <p>Go to Advanced &gt; Options.<br/>         Disable (uncheck) SIP.<br/>         Disable (uncheck) RTSP.<br/>         Click Apply.</p>   |
| <p><b>Ubiquiti</b></p>   | <p>Use the configuration tree if supported: system -&gt; conntrack -&gt; modules -&gt; sip -&gt; disable</p> <p>Alternatively, you can SSH into the device and run the following commands:</p> <pre>configure set system conntrack modules sip disable commit save exit</pre>  |
| <p><b>Virgin SuperHub</b></p>  | <p>SIP ALG cannot be disabled in the settings of SuperHubs.<br/>         Please see our workarounds at the top of the page.</p>  |
| <p><b>Vodafone</b></p>   | <p>2018 Onwards - See Huawei (HHG2500)</p>   |

|  |  |
|--|--|
| <p><b>Vyatta / Brocade:</b></p>          | <p>Type the following into the CLI</p> <pre>configure set system conntrack modules sip disable commit save exit</pre>  |
| <p><b>Watchguard Firewall</b></p>        | <p>Detailed instructions can be found here: <a href="https://www.voicehost.co.uk/help/watchguard-firewall-sip-configuration">https://www.voicehost.co.uk/help/watchguard-firewall-sip-configuration</a></p>  |
| <p><b>ZyXEL</b></p>                      | <p>Under Network or Advanced -&gt; ALG un-tick the options Enable SIP ALG and Enable SIP Transformations. Telnet commands must be used to disable SIP ALG with some other Zyxel routers.</p> <ol style="list-style-type: none"> <li>1. Telnet into the router.</li> <li>2. Select menu items 24 then 8.</li> <li>3. To display the current SIP ALG status run the following command:</li> <li>4. ip nat service sip active</li> <li>5. To turn off SIP ALG:</li> <li>6. ip nat service sip active 0</li> </ol> |
| <p><b>ZyXEL (ZyWALL USG Routers)</b></p> | <p>Go to Settings &gt; Configuration &gt; Network &gt; ALG.<br/>         Disable SIP ALG.<br/>         Turn ON Enable SIP Transformations.<br/>         Turn OFF Enable Configure SIP Inactivity Timeout.</p>  |