

# CLOUD PHONE PRO

## Recomendações de Firewall

e informações sobre SIP ALG



### Índice

<b>Apresentação</b>	<b>3</b>
<b>Pré-requisitos de rede</b>	<b>3</b>
<b>Firewalls</b>	<b>4</b>
Portas de firewall para liberação no cliente	4
Configurações adicionais Firewall FortGate	7
Configurações adicionais Firewall SONICWALL	13
Recomendações para Antivírus	13
<b>SIP ALG</b>	<b>14</b>
O que é o SIP ALG?	14
Muitos roteadores têm o SIP ALG ativado por padrão.	14
Como isso pode afetar a telefonia?	14
Desativei o SIP ALG, mas ainda estou com problemas...	15
Como desativo o SIP ALG?	16

# Apresentação

O correto funcionamento dos ramais do CloudPhone Pro dependem de alguns pré-requisitos de rede que precisam ser atendidos para evitar falhas no funcionamento dos ramais. O presente documento tem o objetivo de detalhar todas as orientações para que os ramais funcionem corretamente nas redes das empresas e residências. Todas as redes possuem equipamentos que são conhecidos como firewalls e/ou roteadores que possuem configurações que podem impactar no funcionamento dos ramais. Este documento apresenta os pré-requisitos e detalha configurações de alguns fabricantes. Caso o seu equipamento não esteja nesta lista, siga as orientações da sessão pré-requisitos e configure de acordo com o que está sendo recomendado.

## Pré-requisitos de rede

As redes de domésticas e empresariais possuem muitas variáveis e formas de serem configuradas, podendo afetar o funcionamento e a qualidade dos serviços de voz. Para que o serviço de Voz funcione corretamente, existe um conjunto de requisitos mínimos que a rede do cliente precisa atender para garantir que o serviço funcione conforme esperado.

Abaixo está um resumo desses requisitos:

- ▶ O firewall precisa liberar o acesso às portas HTTP 80 e HTTPS 443;
- ▶ O roteador/ firewall do cliente não deve manipular os pacotes SIP ou RTP na camada de aplicação. Se qualquer roteador possui a funcionalidade SIP Access Layer Gateway (ALG), esta deve ser desativada, conforme recomendações do tópico SIP ALG deste documento;
- ▶ A largura de banda da Internet do cliente deve ser dimensionada para permitir a quantidade mínima de largura de banda de dados necessária mais o número total de chamadas de voz simultâneas exigidas pelo local;
- ▶ As liberações de firewall devem seguir as recomendações detalhadas no tópico Firewall do presente documento;
- ▶ A rede local (LAN) do cliente deve ser dimensionada para permitir a quantidade máxima de largura de banda de dados necessária mais o número total de chamadas de voz simultâneas exigidas pelo local.

## Firewall

### Portas de firewall para liberação no cliente

Para realizar a implantação da solução é necessário que as portas abaixo estejam liberadas para os usuários externos:

Origem	Destino	Porta	Transporte	Direção	Descrição
Rede Cliente	45.63.1.46	80/443	TCP	Bi-direcional	License
Rede Cliente	189.112.195.169	5060/5061/5080	UDP & TCP	Bi-direcional	Sinalização SIP
Rede Cliente	187.72.201.43	5060/5061/5080	UDP & TCP	Bi-direcional	Sinalização SIP
Rede Cliente	189.112.195.169	10000 - 65535	UDP & TCP	Bi-direcional	RTP VoIP
Rede Cliente	187.72.201.43	10000 - 65535	UDP & TCP	Bi-direcional	RTP VoIP
Rede Cliente	187.72.201.30	80/443	TCP	Bi-direcional	HTTP/HTTPs
Rede Cliente	187.72.201.31	80/443	TCP	Bi-direcional	HTTP/HTTPs
Rede Cliente	187.72.201.31	5280/5222/5422	TCP	Bi-direcional	Chat
Rede Cliente	187.72.201.32	10000 a 65535	UDP & TCP	Bi-direcional	RTP WebRTC
Rede Cliente	187.72.201.32	80/443	TCP	Bi-direcional	WebRTC
Rede Cliente	187.72.201.40	80/443	TCP	Bi-direcional	OmniPro
Rede Cliente	187.72.201.40	10000 a 65535	UDP & TCP	Bi-direcional	OmniPro

## Firewall e SIP ALG

<b>Rede Cliente</b>	187.72.201.41	80/443	TCP	Bi-direcional	WebRTC
<b>Rede Cliente</b>	187.72.201.41	10000 a 65535	UDP & TCP	Bi-direcional	RTP WebRTC
<b>Rede Cliente</b>	187.72.201.45	5060/5061/5080	UDP & TCP	Bi-direcional	Sinalização SIP
<b>Rede Cliente</b>	187.72.201.45	10000 a 65535	UDP & TCP	Bi-direcional	RTP vSession

Origem	Destino	Porta	Transporte	Direção	Descrição
<b>Rede Cliente</b>	dps.digivox.com.br	443/80	TCP	Bi-direcional	Unity License
<b>Rede Cliente</b>	ucpro.algartelem.com.br	443/80	TCP	Bi-direcional	Unity
<b>Rede Cliente</b>	webrtc.ucpro.algartelem.com.br	443/80	TCP	Bi-direcional	WebRTC
<b>Rede Cliente</b>	webrtc2.ucpro.algartelem.com.br	443/80	TCP	Bi-direcional	WebRTC
<b>Rede Cliente</b>	contact.ucpro.algartelem.com.br	5060/5061 5080	UDP/TCP	Bi-direcional	SIP
<b>Rede Cliente</b>	contact2.ucpro.algartelem.com.br	5060/5061 5080	UDP/TCP	Bi-direcional	SIP
<b>Rede Cliente</b>	contact.ucpro.algartelem.com.br	10000 a 65535	UDP	Bi-direcional	RTP
<b>Rede Cliente</b>	contact2.ucpro.algartelem.com.br	10000 a 65535	UDP	Bi-direcional	RTP

## Firewall e SIP ALG

---

<b>Rede Cliente</b>	omni.algartelem.com.br	443/80/5280/ 5222/5422	TCP	Bi-direcional	Omni
<b>Rede Cliente</b>	chat.ucpro.algartelem.com.br	443/80/5280/ 5222/5422	TCP	Bi-direcional	Chat
<b>Rede Cliente</b>	public-chat.ucpro.algartelem.com.br	443/80/5280/ 5222/5422	TCP	Bi-direcional	Chat
<b>Rede Cliente</b>	upload-chat.ucpro.algartelem.com.br	443/80/5280/ 5222/5422	TCP	Bi-direcional	Chat
<b>Rede Cliente</b>	upload-public-chat.ucpro.algartelem.com.br	443/80/5280/ 5222/5422	TCP	Bi-direcional	Chat

### Complementares

Origem	Destino	Porta	Transporte	Direção	Descrição
Rede Cliente	webrtc2.ucpro.algartelecom.com.br	3478/5349	UDP/TCP	Bi-direcional	STUN
Rede Cliente	app.squad.us	80/443	TCP	Bi-direcional	Squad
Rede Cliente	update.squad.us	80/443	TCP	Bi-direcional	Squad
Rede Cliente	gstaticadssl.l.google.com	80/443	TCP	Bi-direcional	API
Rede Cliente	update.googleapis.com	80/443	TCP	Bi-direcional	API
Rede Cliente	s3-1-w.amazonaws.com	80/443	TCP	Bi-direcional	API

Origem	Destino	Porta	Transporte	Direção	Descrição
Rede Cliente	187.72.201.41	3478/5349	UDP/TCP	Bi-direcional	STUN
Rede Cliente	100.27.36.199	80/443	TCP	Bi-direcional	Squad
Rede Cliente	172.217.28.131	80/443	TCP	Bi-direcional	Squad
Rede Cliente	172.217.29.3	80/443	TCP	Bi-direcional	API

Uma recomendação geral para firewalls de diversos fabricantes, é estender a sessão UDP para 5min assim os ramais registrados em UDP conseguem enviar REGISTER dentro dessa janela, garantindo que os mesmos permaneçam registrados, dando estabilidade no uso da ferramenta. Alguns firewalls dispõem de configurações de SIP Helper que fazem essa extensão da sessão UDP, porém voltada só ao protocolo SIP.

### Configurações adicionais Firewall FortGate

- 1 - Criar uma política específica para a comunicação do Cloudphone;
- 2 - Alterar o tempo de sessão para conexões com o SBC do CloudPhone;
- 2 - Desativar a utilização de ASIC, caso o firewall possua esta funcionalidade;
- 3 - Limpar as sessões destinadas ao CloudPhone.

Realizar a criação de uma política específica para o IP/FQDN do SBC do CloudPhone liberando as portas necessárias para a comunicação, ou todas as portas e protocolos, e via linha de comando alterar o tempo de sessão da política para 12h e desativar a opção auto-asic-offload.

#### Exemplo de configuração:

```
config firewall policy
edit <id>
    set srcintf "ZN_LAN"
    set dstintf "virtual-wan-link"
    set srcaddr "all"
    set dstaddr 189.112.195.169/32-Cloudphone
    set action accept
    set schedule "always"
    set service "ALL"
    set auto-asic-offload disable
```

## Firewall e SIP ALG

---

```
set session-ttl 43200
```

```
set nat enable
```

```
next
```

```
end
```

```
diagnose sys session filter dst 189.112.195.169
```

```
diagnose sys session clear
```

## Firewall e SIP ALG

---

Sugestão do processo de implementação:

Página de apoio:

<https://www.voicehost.co.uk/help/sip-alg-and-why-it-should-be-disabled-your-router>

**Check the session helpers enabled on the FortiGate by using the CLI as shown below.**

```
FG200B3909600137 # show system session-helper
config system session-helper
```

**To disable a session-helper simply delete the id of the session-helper by running the following CLI command:**

```
FG200B3909600137 (session-helper) # delete ?
<tableid> please input an int id. 0 means the lowest available id.
```

**A second step is required to fully disable a SIP session-helper, enter the following CLI command:**

```
FG200B3909600137 (settings) # set sip-helper ?
disable disable
enable enable
FG200B3909600137 (settings) # set sip-helper disable
FG200B3909600137 (settings) # end
```

### 1) Removing the session helper.

Run the show command under system session-helper:

```
#config system session-helper
```

```
show
```

Among the displayed settings will be one similar to the following example:

```
#edit 13
```

```
set name sip
```

```
set protocol 17
```

```
set port 5060
```

```
next
```

## Firewall e SIP ALG

---

Here entry 13 is the one which points to SIP traffic which uses UDP port 5060 for signaling.

In this example, the next commands to remove the corresponding entry would be:

```
#delete 13  
  
end
```

**Note** It is not necessary for the SIP entry to be, so crosscheck which entry has the sip helper settings.

### 2) Change the default `-voip -alg-mode`.

Run the following commands:

```
#config system settings  
  
    set default-voip-alg-mode kernel-helper-based  
  
    set sip-helper disable  
  
    set sip-nat-trace disable  
  
end
```

By default, the default-voip-alg-mode is set to proxy-based.

**IMPORTANT Note** Since version 6.2.2. the CLI commands are different:

```
#config system settings  
  
    set default-voip-alg-mode kernel-helper-based  
  
    set sip-expectation disable  
  
    set sip-nat-trace disable  
  
end  
  
#config voip profile  
  
edit default  
  
show
```

## Firewall e SIP ALG

---

```
config sip
show
set status disable
set strict-register disable
end
next
end
```

**The last set of commands disables processing of RTP protocol on the firewall**

```
#config voip profile
edit default
config sip
set rtp disable
end
end
```

Special Note Disabling SIP session helper with VDOMs enabled.

**If VDOMs are enabled, disable the session helper from global as the session helper setting is a global parameter and is not available under any particular VDOM.**

```
FGT# config global
FGT(global)# config system session-helper
```

**In such cases the below settings can be used:**

```
FGT# config firewall service custom
FGT(custom)#edit Helper-disable
FGT(Helper-disable)# set protocol IP
FGT(Helper-disable)# set helper disable
FGT(Helper-disable)# end
```

3) Either clear sessions or reboot to make sure changes take effect

a) To clear sessions

#diagnose system session filter ...

#diagnose system session clear

b) To reboot

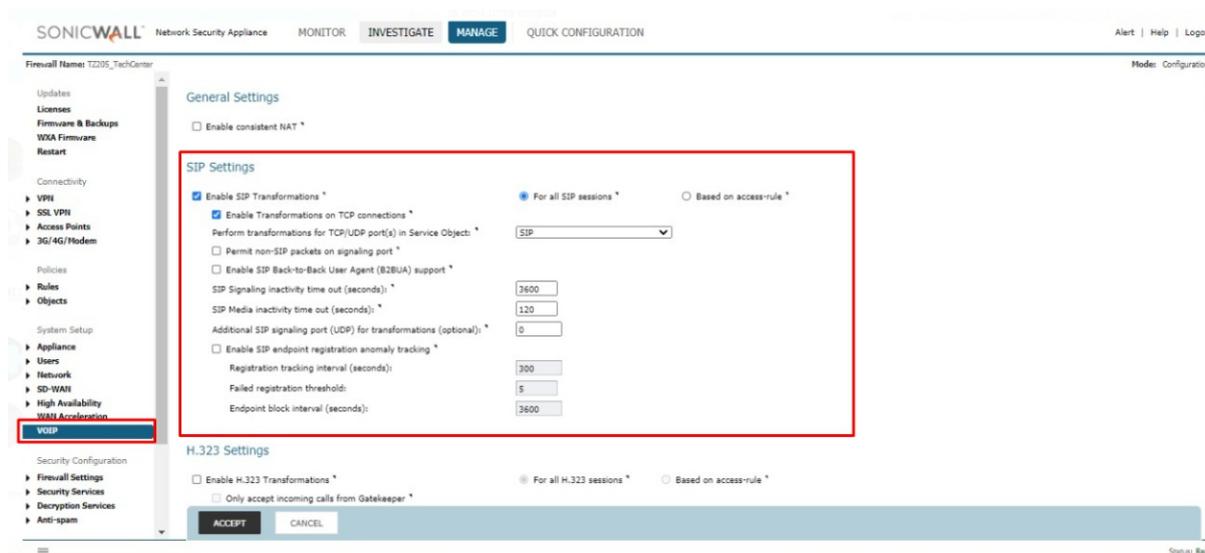
#execute reboot

# Configurações adicionais Firewall SONICWALL

Para firewalls SONICWALL as configurações abaixo também devem estar habilitadas:

Sonicwall habilitar SIP Transformations

Manage -> VoIP -> SIP Settings



## Recomendações para Antivírus

Para os softwares de antivírus recomendamos que libere as URLs descritas acima além de liberar (ou criar uma exceção) para o APP Desktop, a partir do diretório "C:\Program Files\Algar" assim a liberação é feita para o executável, suas bibliotecas e DLLs.

# SIP ALG

## 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 escrever 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 a telefonia?

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**

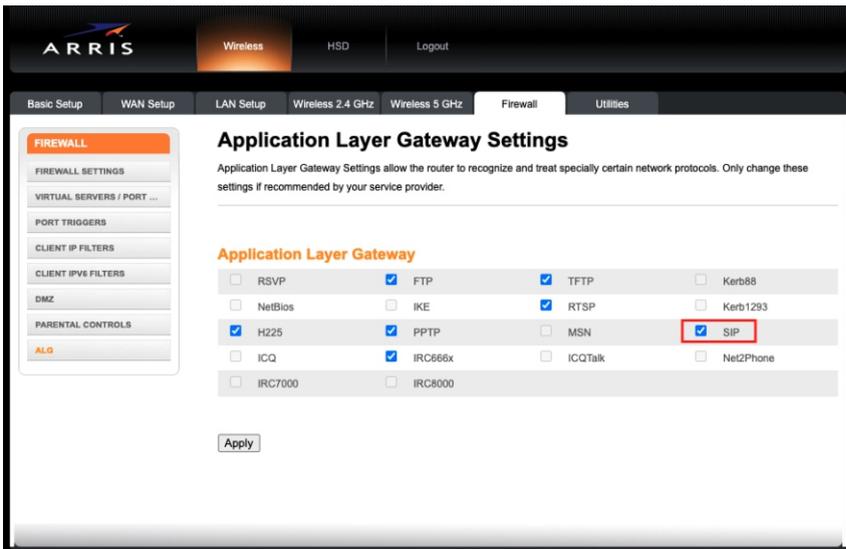
Se você ainda estiver tendo problemas após desativar o SIP ALG, verifique sua configuração de firewall.

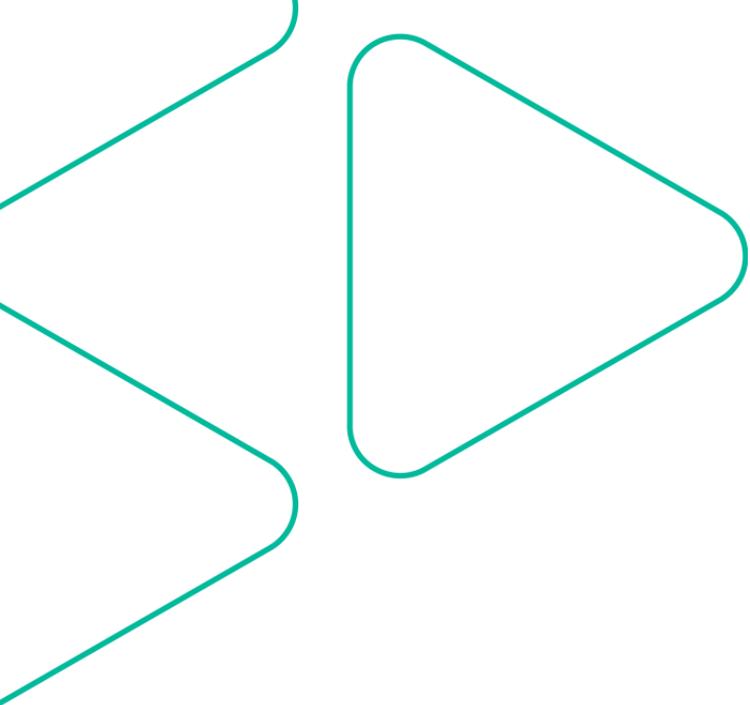
### Como desativo o SIP ALG?

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.

Abaixo está uma lista de roteadores e como desativar em cada um deles. Caso o seu roteador não esteja na lista abaixo, o site <https://www.voip-info.org/routers-sip-alg/> mantém uma lista de roteadores de fabricantes comuns de mercado com detalhes sobre como desativar o SIP ALG nestes equipamentos e você pode consultar neste site.

<b>Firewalls Barracuda</b>	Acesse Firewall > Firewall Rules > Custom Firewall Access Rules Clique em "Disabled" no check próximo às regras com nomes LAN-2-INTERNET-SIP e INTERNET-2- LAN-SIP Isto irá desabilitar o SIP ALG.
<b>D-Link</b>	Em Configurações 'Avançadas' --> Configuração 'Application Level Gateway (ALG)' desmarque a opção 'SIP'.
<b>Fortinet</b>	Fortigate: Desabilitando o SIP ALG no perfil VoIP SIP é habilitado por padrão no perfil VoIP. Desabilite com o seguinte comando: <code>config voip profile</code> <code>edit VoIP_Pro_2</code> <code>config sip</code> <code>set status disable</code> <code>end</code>
<b>Linksys</b>	Verifique pela opção SIP ALG em Administração, na aba Avançado. Você precisará desabilitar também a opção SPI no Firewall.
<b>Mikrotik</b>	Desabilite o SIP Helper
<b>Netgear</b>	Procure por 'SIP ALG' nas configurações 'WAN'. Em 'NAT Filtering' desmarque a opção 'SIP ALG' Port Scan e DoS Protection.
<b>Firewall SonicWALL</b>	Na aba VoIP, a opção 'Enable Consistent NAT' precisa estar habilitada e 'Enable SIP Transformations' desabilitada.
<b>TP-Link</b>	Acesse a interface web do seu roteador.

	<p>Geralmente o usuário e senha padrão do TP-Link é admin/admin.          Clique em Configurações avançadas, em seguida clique em NAT e clique em ALG.          Desmarque a opção SIP Enabled. (Alguns firmwares do TP-Link exibe como SIP Transformations que é a mesma funcionalidade).          Clique em Salvar/aplicar.</p>
<p><b>Ubiquiti</b></p>	<p>Utilize a árvore de configuração se seu equipamento tem suporte:          system -&gt; contrack -&gt; modules -&gt; sip -&gt; disable</p> <p>Alternativamente, você pode acessar via SSH e usar os comandos abaixo:          configure          set system contrack modules sip disable          commit          save          exit</p>
<p><b>Modem NET Arris TG1692A</b></p>	<p>Embaixo do modem existe uma etiqueta que possui o usuário e senha de acesso ao modem.          Digite o endereço do modem no Browser, geralmente é o 192.168.0.1 e faça login com o usuário e senha.</p> <p>Acesse a sessão Firewall &gt; ALG e desabilite o SIP:</p>  <p>The screenshot shows the 'Application Layer Gateway Settings' page in the Arris modem's web interface. The 'Firewall' tab is selected, and the 'ALG' sub-tab is active. Under 'Application Layer Gateway', several protocols are listed with checkboxes. The 'SIP' checkbox is checked and highlighted with a red box. Other checked protocols include H225, PPTP, and FTP. Other protocols like RSVP, NetBios, IKE, MSN, ICQ, IRC7000, IRC8000, TFTP, RTSP, Kerb88, Kerb1293, and Net2Phone are unchecked.</p>



**Algar**   
Telecom

DIGIVO ><

