SIP session helper / ALG

Starting @ 1:30pm
Who am I?

• David Attias
• Installing VoIP systems for over 11 years
• Owner of Penny Tone LLC
• Mikrotik user for 6 years
• Mikrotik Trainer
  MTCNA, MTCRE & MTCWE
Purpose of this lecture

To inform Mikrotik users on the purpose and functions of SIP ALG.
1- What is ALG & what does it do.
2- The problem with VoIP and NAT
3- When is SIP ALG necessary and unnecessary?
4- How SIP ALG corrects problems.
5- Testing with wireshark
6- SIP ALG Timeout
7- SIP ALG direct-media
WHAT IS ALG?
WHAT IS ALG?

- **Application Layer Gateway**
- A **Gateway** (firewall) that re-writes specific Application Layer data fields.
- ALG is a firewall feature that rewrites Layer 7 data for specific applications.
Keep in mind

- Only applies to NAT translation rules.
- NAT’ed devices are unaware that ALG is changing anything.
- Also known as:
  - NAT helper (Linux)
  - NAT session helper
  - SIP Transformations
  - Service ports
The Problem with VoIP and NAT
The Problem with VoIP and NAT

- SIP servers need to know the IP of all registered phones.
- Phones register their locally configured IP with the SIP server.
- If the phone and server are in the same network, no problems.
- If the phone is behind NAT and reports its IP to a remote server, the server responses will NOT be able to reach the phone.
The Result

- Phone can not receive calls
- One way audio
What ALG Does.
What ALG Does.

- ALG does exactly the same thing NAT translation does, but at layer 7.
- ALG intercepts the application messages before they leave the router.
- Then inspects and replaces the “private client ip:port” with the “public ip:port” of the router (nat rule).
Dear SIP Server,
I’ve been thinking about you and I want to INVITE you to SIP and RTP with me. Contact 192.168.20.100
Dear SIP Server,
I’ve been thinking about you and I want to INVITE you to SIP and RTP with me.
Contact 192.168.20.100
75.142.151.49
ALG WAS HERE
Basic terms
SIP and SDP

- SIP and SDP are VoIP Layer 7 protocols
- SIP – Session Initiated Protocol are commands exchanged between sip devices (register, invite, trying, hold, xfer, bye)
- SDP – Session Description Protocol is information about the audio (RTP) stream of a call.
RouterOS SIP ALG settings
RouterOS SIP ALG options

/ip firewall service-port

**Ports:**
- Remote Sip Server listening port. default values are 5060, 5061
- Applies to TCP and UDP
- Single port, no ranges
- Up to 8 entries

**Sip-direct-media**
- Allows a redirect of the RTP media stream to go directly from sip device to sip device
- Default value is yes.

**Timeout:**
- Sets the sip UDP timeout in connection tracker.
- Default is 1 hour

**Mikrotik CLI**
/ip firewall service-port
set sip ports=5060,5061 sip-direct-media=yes sip-timeout=01:00:00 disabled=no
How does ALG correct SIP problems?
How does ALG correct SIP problems?

- By replacing specific private IP:port with router’s wan side IP:port

ALG changes:
SIP headers: Via, Contact
SDP Body: m= o= c=

- ALG makes changes to Layer 7 data transparently as it passes through the NAT rule.
Layer 7 data before and after (with ALG enabled)
SIP REGISTER message BEFORE ALG modification:

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-8fb0e171
From: "David Attias" <sip:201525@207.252.1.148>;tag=191914b06be00
To: "David Attias" <sip:201525@207.252.1.148>
Call-ID: 6894e30c-h1c8d357@192.168.20.100
CSeq: 1373 REGISTER
Max-Forwards: 70
Contact: "David Attias" <sip:201525@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

The fields ALG will change
SIP REGISTER message AFTER ALG modification:

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 75.142.151.49:1024;branch=z9hG4bK-8fb0e171
From: "David Attias" <sip:525@207.252.1.148>;tag=191914b06be0
To: "David Attias" <sip:525@207.252.1.148>
Call-ID: 6894e30c-h1c8d357@192.168.20.100
CSeq: 1373 REGISTER
Max-Forwards: 70
Contact: "David Attias" <sip:525@75.142.151.49:1024>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

After ALG
The “respond to” IP and port
Layer 7 Data with before ALG

INVITE sip:*98@207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-7badf56d
From: "David Attias" <sip:525@207.252.1.148>;tag=f95367fa52060ce500
To: "Voice Mail" <sip:*98@207.252.1.148>
Call-ID: 9c8a315e-419d32d1@192.168.20.100
CSeq: 101 INVITE
Max-Forwards: 70
Contact: "David Attias" <sip:525@192.168.20.100:5060>
Expires: 240
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 397
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
Content-Type: application/sdp

SIP Headers

Before ALG modifies layer 7 data

SDP Body

v=0
o=176664 176664 IN IP4 192.168.20.100
s=-
c=IN IP4 192.168.20.100
t=0 0
m=audio 14254 RTP/AVP 0 2 8 9 18 96 97 98 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtpmap:2 G726-32/8000
a=fmtp:101 0-15
a=ptime:30
a=sendrecv
 INVITE sip:*98@207.252.1.148 SIP/2.0
 Via: SIP/2.0/UDP 75.142.151.49:1024;branch=z9hG4bK-7badf56d
 From: "David Attias" <sip:525@75.142.151.49>;tag=f95367fa52060ce500
 To: "Voice Mail" <sip:*98@207.252.1.148>
 Call-ID: 9c8a315e-419d32d1@192.168.20.100
 CSeq: 101 INVITE
 Max-Forwards: 70
 Contact: "David Attias" <sip:525@75.142.151.49:1024>
 Expires: 240
 User-Agent: Cisco/SPA504G-7.6.2b
 Content-Length: 397
 Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
 Supported: replaces
 Content-Type: application/sdp

v=0
o= 176664 176664 IN IP4 75.142.151.49
s=-
c=IN IP4 75.142.151.49
t=0 0
m=audio 19032 RTP/AVP 0 2 8 9 18 96 97 98 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=rtpmap:2 G726-32/8000
a=fmtp:101 0-15
a=ptime:30
a=sendrecv

SIP Headers
After ALG modifies layer 7 data
SDP Body
When is SIP ALG necessary?
When is SIP ALG necessary?

When the SIP device behind NAT is NOT NAT aware
Some SIP devices are not NAT aware and write their (private) device IP in layer 7 messages to the server.

The remote SIP server receives the layer 7 message which specifies a private reply address.

The server sends replies to the private address, which can never be reached.
SIP servers that are not “NAT Aware”

***The public server can receive data, but reply packets are dropped.***

Penny Tone LLC - www.pennytone.com
Example of a SIP device that is not NAT aware
Private / NAT

X100
192.168.20.100
SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032
SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032
SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032

ALG IS required here
With RouterOS SIP ALG enabled
SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032
SIP headers
Via: 75.142.151.49
Contact: 75.142.151.49

SDP Body
o = IN IP4 75.142.151.49
c = IN IP4 75.142.151.49
m = audio 19032

Private / NAT
X100
192.168.20.100

WAN 75.142.151.49
ALG Enabled
Is your SIP device NAT Aware?

- Packet capture in routerOS
  - Capture packets before and after they get modified by ALG
- Decode the capture files in Wireshark
Setting up the packet capture
Before ALG modifications pcap

/tool sniffer
Before ALG modifications pcap

`/tool sniffer`
`set only-headers=no file-name=before-ALG.pcap file-limit=4096`
Before ALG modifications pcap

/tool sniffer
set only-headers=no file-name=before-ALG.pcap file-limit=4096  filter-interface=vlan20 filter-ip-address=192.168.20.100/32 filter-direction=any
Before ALG modifications pcap

/tool sniffer
set only-headers=no file-name=before-ALG.pcap file-limit=4096 filter-interface=_vlan20 filter-ip-address=192.168.20.100/32 filter-direction=any

start
Generate some traffic while the sniffer is capturing packets.
Before ALG modifications pcap

Make sure to stop the sniffer

/tool sniffer

stop
Download pcap files
### Decode in wireshark

<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source Address</th>
<th>Destination Address</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.00000006</td>
<td>192.168.20.1</td>
<td>192.168.20.100</td>
<td>DHCP</td>
<td>357</td>
<td>DHCP Offer - Transaction ID 0xbed323ae</td>
</tr>
<tr>
<td>2</td>
<td>1.003062</td>
<td>192.168.20.1</td>
<td>192.168.20.100</td>
<td>DHCP</td>
<td>357</td>
<td>DHCP ACK - Transaction ID 0xbed323ae</td>
</tr>
<tr>
<td>3</td>
<td>1.688350</td>
<td>192.168.20.100</td>
<td>192.168.20.1</td>
<td>DNS</td>
<td>72</td>
<td>Standard query 0x0001 A pool.ntp.org</td>
</tr>
<tr>
<td>4</td>
<td>1.702269</td>
<td>192.168.20.100</td>
<td>192.168.20.1</td>
<td>DNS</td>
<td>136</td>
<td>Standard query response 0x0001 A pool.ntp.org A.</td>
</tr>
<tr>
<td>5</td>
<td>1.703640</td>
<td>192.168.20.100</td>
<td>208.75.80.4</td>
<td>NTP</td>
<td>90</td>
<td>NTP Version 3, client</td>
</tr>
<tr>
<td>6</td>
<td>1.706975</td>
<td>192.168.20.100</td>
<td>192.168.20.1</td>
<td>TFTP</td>
<td>93</td>
<td>Read Request, File: SEPECE1A9CDAA7D.cnf.xml, Tr...</td>
</tr>
<tr>
<td>7</td>
<td>1.707186</td>
<td>192.168.20.1</td>
<td>192.168.20.100</td>
<td>ICMP</td>
<td>121</td>
<td>Destination unreachable (Port unreachable)</td>
</tr>
<tr>
<td>8</td>
<td>1.708256</td>
<td>192.168.20.100</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>74</td>
<td>1024 - 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1456 W...</td>
</tr>
<tr>
<td>9</td>
<td>1.726556</td>
<td>208.75.80.4</td>
<td>192.168.20.1</td>
<td>NTP</td>
<td>99</td>
<td>NTP Version 3, server</td>
</tr>
<tr>
<td>11</td>
<td>2.087226</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>524</td>
<td>Request: REGISTER sip:207.252.1.148 (1 binding...</td>
</tr>
<tr>
<td>12</td>
<td>2.088547</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>580</td>
<td>Status: 401 Unauthorized</td>
</tr>
<tr>
<td>13</td>
<td>2.293030</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>678</td>
<td>Request: REGISTER sip:207.252.1.148 (1 binding...</td>
</tr>
<tr>
<td>14</td>
<td>2.296426</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>601</td>
<td>Request: OPTIONS sip:100@192.168.20.100:5060</td>
</tr>
<tr>
<td>15</td>
<td>2.296603</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>599</td>
<td>Status: 200 OK (1 binding)</td>
</tr>
<tr>
<td>16</td>
<td>2.297538</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>605</td>
<td>Request: NOTIFY sip:100@192.168.20.100:5060</td>
</tr>
<tr>
<td>17</td>
<td>2.341624</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>460</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>18</td>
<td>2.352654</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>367</td>
<td>Status: 200 OK</td>
</tr>
<tr>
<td>20</td>
<td>5.308726</td>
<td>192.168.20.100</td>
<td>255.255.255.255</td>
<td>UDP</td>
<td>70</td>
<td>55656 -&gt; 55656 Len=28</td>
</tr>
<tr>
<td>21</td>
<td>6.706857</td>
<td>192.168.20.100</td>
<td>192.168.20.1</td>
<td>TFTP</td>
<td>93</td>
<td>Read Request, File: SEPECE1A9CDAA7D.cnf.xml, Tr...</td>
</tr>
<tr>
<td>22</td>
<td>6.708229</td>
<td>192.168.20.1</td>
<td>192.168.20.100</td>
<td>ICMP</td>
<td>121</td>
<td>Destination unreachable (Port unreachable)</td>
</tr>
<tr>
<td>23</td>
<td>7.348782</td>
<td>192.168.20.100</td>
<td>192.168.20.1</td>
<td>TCP</td>
<td>74</td>
<td>[TCP Retransmission] 1024 - 80 [SYN] Seq=0 Win=...</td>
</tr>
</tbody>
</table>

- Frame 19: 56 bytes on wire (448 bits), 56 bytes captured (448 bits)
- Internet Group Management Protocol
### Decode in Wireshark

#### Frame 18
- **Size**: 367 bytes on wire (2936 bits), 367 bytes captured (2936 bits)
- **User Datagram Protocol**: Src Port: 5660 (5660), Dst Port: 5660 (5660)
- **Session Initiation Protocol**

#### SIP Packets
<table>
<thead>
<tr>
<th>Time</th>
<th>Source IP</th>
<th>Destination IP</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.00</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>524</td>
<td>Request: REGISTER sip:207.252.1.148 (1 binding)</td>
</tr>
<tr>
<td>12.00</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>580</td>
<td>Status: 401 Unauthorized</td>
</tr>
<tr>
<td>13.00</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>678</td>
<td>Request: REGISTER sip:207.252.1.148 (1 binding)</td>
</tr>
<tr>
<td>14.00</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>601</td>
<td>Request: OPTIONS sip:100@192.168.20.100:5060</td>
</tr>
<tr>
<td>15.00</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>509</td>
<td>Status: 200 OK (1 binding)</td>
</tr>
<tr>
<td>16.00</td>
<td>207.252.1.148</td>
<td>192.168.20.100</td>
<td>SIP</td>
<td>505</td>
<td>Request: NOTIFY sip:100@192.168.20.100:5060</td>
</tr>
<tr>
<td>17.00</td>
<td>192.168.20.100</td>
<td>207.252.1.148</td>
<td>SIP</td>
<td>460</td>
<td>Status: 200 OK</td>
</tr>
</tbody>
</table>
Decode in wireshark
Decode in wireshark

Wireshark · Follow UDP Stream (udp.stream eq 4) · before-ALG

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-eeffdbff
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-eeffdbff;received=207.252.1.145
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Server: FF-PBX-13.0.196.19(13.15.8)
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO,
PUBLISH, MESSAGE
Supported: replaces, timer
WWW-Authenticate: Digest algorithm=MD5, realm="asterisk", nonce="01a48834"
Content-Length: 0

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-e9fcb8df
From: "100" <sip:100@207.252.1.148>;tag=36d71bb091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf0b-e1cc0d64@192.168.20.100
CSeq: 60160 REGISTER
Max-Forwards: 70

4 client pkt(s), 2 server pkt(s), 4 turns.

Entire conversation (14 kB)
207.252.1.148:5060 → 192.168.20.100:5060 (4428 bytes)
192.168.20.100:5060 → 207.252.1.148:5060 (9940 bytes)
Decode in Wireshark
If your SIP device is not NAT Aware
Enable SIP ALG!
Enable SIP ALG
Enable SIP ALG

/ip firewall service-port enable sip
capture packets after ALG modification
After ALG modifications pcap

/tool sniffer
After ALG modifications pcap

/tool sniffer
set only-headers=no file-name=after-ALG.pcap file-limit=4096
After ALG modifications pcap

/tool sniffer
set only-headers=no file-name=after-ALG.pcap file-limit=4096 filter-interface=ether1-gateway filter-ip-address=207.252.1.148/32 filter-port=5060 filter-direction=any
After ALG modifications pcap

/tool sniffer
set only-headers=no file-name=after-ALG.pcap file-limit=4096 filter-interface=ether1-gateway
filter-ip-address=207.252.1.148/32 filter-port=5060 filter-direction=any

start
Generate some traffic while the sniffer is capturing packets.
After ALG modifications pcap

Make sure to stop the sniffer

/tool sniffer

stop
Download pcap files
Decode in Wireshark

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.148:1024;branch=z9hG4bK-82c1a276
From: "100" <sip:100@207.252.1.148>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.148>
Call-ID: e68aae97-897b8a71@192.168.20.100
CSeq: 18716 REGISTER
Max-Forwards: 70
Contact: "100" <sip:100@207.252.1.145:1024>; expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-3586ccde
From: "100" <sip:100@207.252.1.148>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.148>
Call-ID: e68aae97-897b8a71@192.168.20.100
CSeq: 18717 REGISTER
Max-Forwards: 70
Authorization: Digest
username="100", realm="asterisk", nonce="6c01b3a5", url="sip:207.252.1.148", algorithm=MD5, response="81d37d55728c12cd6ef39e01d6ee928d"
Contact: "100" <sip:100@207.252.1.145:1024>; expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
ALG Enabled

Before modification & after modification

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-eeffddbff
From: "100" <sip:100@207.252.1.148>;tag=36d71b091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf9b-e1cc0d64@192.168.20.100
CSeq: 60159 REGISTER
Max-Forwards: 70
Content-Length: 0
User-Agent: Cisco/SPA504G-7.6.2b
Supported: replaces
Expires: 3600

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100;branch=z9hG4bK-e9fc8df
From: "100" <sip:100@207.252.1.148>;tag=36d71b091995583o1
To: "100" <sip:100@207.252.1.148>
Call-ID: 6593bf9b-e1cc0d64@192.168.20.100
CSeq: 60160 REGISTER
Max-Forwards: 70
Authorization: Digest username="100",realm="asterisk",nonce="01a48834",algorithm=MD5,response="36c61d31d35e832641b34b782b" 
Content-Length: 0
User-Agent: Cisco/SPA504G-7.6.2b
Supported: replaces
Expires: 3600
```

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-82c1a276
From: "100" <sip:100@207.252.1.145>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.145>
Call-ID: e88ae07-887b8a7l@192.168.20.100
CSeq: 18716 REGISTER
Max-Forwards: 70
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
Expires: 3600
```

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024;branch=z9hG4bK-3586ccde
From: "100" <sip:100@207.252.1.145>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.145>
Call-ID: e88ae07-887b8a7l@192.168.20.100
CSeq: 18717 REGISTER
Max-Forwards: 70
Authorization: Digest username="100",realm="asterisk",nonce="6c91b3a5",url="sip: 207.252.1.145",algorithm=MD5,response="81d37d55728c12cd5e39e01d6ee928d0c" 
Content-Length: 0
User-Agent: Cisco/SPA504G-7.6.2b
Supported: replaces
Expires: 3600
```

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024
From: "100" <sip:100@207.252.1.145>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.145>
Call-ID: e88ae07-887b8a7l@192.168.20.100
CSeq: 18718 REGISTER
Max-Forwards: 70
Authorization: Digest username="100",realm="asterisk",nonce="6c91b3a5",url="sip: 207.252.1.145",algorithm=MD5,response="81d37d55728c12cd5e39e01d6ee928d0c" 
Content-Length: 0
User-Agent: Cisco/SPA504G-7.6.2b
Supported: replaces
Expires: 3600
```

```
REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 207.252.1.145:1024
From: "100" <sip:100@207.252.1.145>;tag=1d8c3b3fa6a8a34co1
To: "100" <sip:100@207.252.1.145>
Call-ID: e88ae07-887b8a7l@192.168.20.100
CSeq: 18719 REGISTER
Max-Forwards: 70
Authorization: Digest username="100",realm="asterisk",nonce="6c91b3a5",url="sip: 207.252.1.145",algorithm=MD5,response="81d37d55728c12cd5e39e01d6ee928d0c" 
Content-Length: 0
User-Agent: Cisco/SPA504G-7.6.2b
Supported: replaces
Expires: 3600
```
```
When is SIP ALG unnecessary?
When is SIP ALG unnecessary?

When the SIP device is NAT aware.

1. Server is behind NAT
2. Server is outside NAT (public server)
When is SIP ALG unnecessary?

SIP servers behind NAT

- Nat aware SIP servers have the option to detect their WAN ip and write it in the SIP/SDP messages where necessary, before sending it.
- FreePBX detects the WAN ip and inserts it in SIP messages where necessary.
Private / NAT

Server
192.168.20.2

WAN
75.142.151.49

SIP headers
Via: 75.142.151.49
Contact: 75.142.151.49

SDP Body
o = IN IP4 75.142.151.49
c = IN IP4 75.142.151.49
m = audio 19032
ALG Disabled

WAN
75.142.151.49

Server
192.168.20.2

SIP headers
Via: 75.142.151.49
Contact: 75.142.151.49

SDP Body
o = IN IP4 75.142.151.49
c = IN IP4 75.142.151.49
m = audio 19032

Private / NAT
Servers outside NAT (public server)
Servers outside NAT (public server)

- SIP servers have NAT options for each extension
Servers outside NAT (public server)

- SIP servers have NAT options for each extension
- If server side extension states NAT=Yes then send all responses to the client originating IP and Port.
Private / NAT

WAN
75.142.151.49

ALG Disabled
WAN 75.142.151.49

ALG Disabled

Private / NAT

X100
192.168.20.100
Sip Server
207.252.1.148

WAN
75.142.151.49

Private / NAT

X100
192.168.20.100

SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032
SIP Server 207.252.1.148

WAN 75.142.151.49

Private / NAT

X100 192.168.20.100

SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032

ALG Disabled
SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032

Private / NAT

X100
192.168.20.100

WAN
75.142.151.49
SIP headers
Via: 192.168.20.100
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 19032
SIP headers
Via: received=75.142.151.49
Contact: 192.168.20.100

SDP Body
o = IN IP4 192.168.20.100
c = IN IP4 192.168.20.100
m = audio 25481

Private / NAT

X100
192.168.20.100
When does ALG break VoIP?
When does ALG break VoIP?

- DOES NOT HAPPEN WITH Mikrotik RouterOS!
- Poor quality ALG’s replace ALL private IP’s in SIP headers, including Call-ID
When does ALG break VoIP?

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-8fb0e171
From: "David Attias" <sip:201525@207.252.1.148>;tag=191914b06be00
To: "David Attias" <sip:201525@207.252.1.148>
Call-ID: 6894e30c-h1c8d357@192.168.20.100
CSeq: 1373 REGISTER
Max-Forwards: 70
Contact: "David Attias" <sip:201525@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces
When does ALG break VoIP?

REGISTER sip:207.252.1.148 SIP/2.0
Via: SIP/2.0/UDP 192.168.20.100:5060;branch=z9hG4bK-8fb0e171
From: "David Attias" <sip:201525@207.252.1.148>;tag=191914b06be00
To: "David Attias" <sip:201525@207.252.1.148>
Call-ID: 6894e30c-h1c8d357@192.168.20.100
CSeq: 1373 REGISTER
Max-Forwards: 70
Contact: "David Attias" <sip:201525@192.168.20.100:5060>;expires=3600
User-Agent: Cisco/SPA504G-7.6.2b
Content-Length: 0
Allow: ACK, BYE, CANCEL, INFO, INVITE, NOTIFY, OPTIONS, REFER, UPDATE
Supported: replaces

NEVER change anything in this field !!!
When does ALG break VoIP?

- DOES NOT HAPPEN WITH RouterOS!
- Poor quality ALG’s replace ALL private IP’s in SIP headers, including Call-ID
- Poor quality ALG’s unnecessarily adds a ; which breaks the syntax of sip requests.
SIP ALG Timeout

The problem:
• The phone sets layer 7 session timeout on the server.

• The router sets the UDP timeout for the session.
SIP ALG Timeout

The problem:
- The phone sets layer 7 session timeout on the server.
- The router sets the UDP timeout for the session.
- If the router session timeout expires before the server session timeout, the server would send data to an expired session (closed return port)
SIP ALG Timeout

The Solution:

- Manually set SIP ALG timeout
- Set it higher than your lowest sip keepalive message interval (register, invite, options)
SIP Direct Media
SIP Direct Media

- Allows a redirect of the RTP media stream to go directly from SIP device to SIP device, “cutting out the middle man”
- The SIP servers are responsible for setting up the direct media stream.
- After the initial call is established the NAT’ed SIP server will re-invite the public media server to establish a direct media connection, bypassing the middle server
Standard Flow

SIP Server

Media (RTP) Server

SIP messages

Media

SIP messages

Private / NAT

Media

SIP messages
Direct-Media
SIP Direct Media

- The sip-direct-media option has the ability to block or allow the NAT’ed server from re-inviting the media server for a direct media session.
  - sip-direct-media yes
    Allows direct media re-invites
  - sip-direct-media no
    Blocks direct media re-invites
Standard Flow

Sip Server

Media (RTP) Server

SIP messages

Media
Re-cap

1- Use SIP ALG when your NAT’ed sip device is NOT NAT aware!
2- Make sure you set your SIP-Server ports correctly
3- Set your UDP timeout higher than your sip keep alive
4- Don’t fear SIP ALG, it’s designed to make your job easier!
Agenda

1. What is ALG & what does it do.
2. The problem with VoIP and NAT
3. When is SIP ALG necessary and unnecessary?
5. Testing with wireshark
6. SIP ALG Timeout
7. SIP ALG direct-media