ND1440 V1.1.1 (2017-03)

NICC Document

Guidance for the use and secure implementation of SIP Application Layer Gateways (ALG)

NICC Standards Limited

The Old Rectory,
Church Street,
Weybridge,
Surrey
KT13 8DE

Tel.: +44(0) 20 7036 3636

Registered in England and Wales under number 6613589

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to NICC. Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by the NICC SIP ALG Task Group.

Introduction

Session Initiation Protocol (SIP) Application Layer Gateway (ALG) / Back to Back User Agent (B2BUA) functionality is often implemented in routers in order to prevent some of the problems that can be caused by Network Address Translation (NAT) and Firewall functions interfering with the SIP traffic. The SIP ALG works by inspecting the SIP traffic at the IP packet layer and, if necessary, modifying it. Many routers have SIP ALG turned on by default.

For the purposes of this ND the SIP ALG is considered to be deployed in such a way that it analyses and potentially modifies all SIP traffic which traverses the router and is therefore not specific to any specific SIP service.

SIP ALG is an example of a signalling/media plane B2BUA as described in section 3.2 of RFC 7092 [2].

Despite SIP ALG being intended to assist with such scenarios as a network of SIP End Points with RFC1918 IP on a LAN behind a router, in many cases it is implemented inconsistently resulting in poor user experience. It has been observed that SIP ALG modifies SIP packets in unexpected ways which gives rise to such issues as SIP endpoints not registering, one way media and incoming calls failing.

The purpose of this ND is to provide information and guidance on the implementation and use of SIP ALG within router devices. This includes -

1. The rationale behind, and the behaviour of, a SIP ALG
2. Scenarios where SIP ALG has been known to cause problems
3. Guidance on enabling and/or disabling SIP ALG
4. Guidance on the impact on IPv6
5. ITSPA SIP ALG Survey Results – See Annex A1 for a summary of the survey results

At the time of writing this ND, no international standards had been published on this topic. This has contributed to inconsistent implementations of SIP ALG, resulting in the inability to deliver Over the Top Hosted Voice Services.

1 Scope

The present document contains guidance on the functionality of SIP ALG as typically deployed in Internet Routers used within business and residential environments.
By following such guidance, Users and Service Providers can better select and configure equipment for SIP based services in a manner that helps mitigate service problems encountered with some SIP ALG implementations.

2 References

For the particular version of a document applicable to this release see ND1610 [1].

2.1 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

[1] ND1610 Next Generation Networks, Release Definition

[2] RFC 7092 A Taxonomy of Session Initiation Protocol (SIP) Back-to-Back User Agents

[3] RFC1918 Address Allocation for Private Internets

2.2 Informative references

None

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and apply:

ALG	An Application Level Gateway acts as an intermediate system between the Internet and the application server that understands the relevant application protocol. It allows customised NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer control/data" protocols such as FTP, SIP, RTSP, etc.
Firewall	A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.
IPv4	Internet Protocol version 4 (IPv4) is the most widely used version of the Internet Protocol, however it has a limited number of addresses, which initially resulted in extended use of NAT.
IPv6	Internet Protocol version 6 (IPv6) is the most recent version of the Internet Protocol (IP) with a much greater address range. It also provides additional benefits but has yet to be widely adopted.
NAT	NAT is a method of remapping one IP address space into another.
SIP ALG	A SIP ALG is intended to manipulate the content of SIP and SDP messages for the correct routeing of media.

3.3 Abbreviations

ALG	Application Layer Gateway
B2BUA	Back to Back User Agent
CP	Communication Provider
CPE	Customer Premises Equipment
FTP	File Transfer Protocol
GUI	Graphical User Interface
IP	Internet Protocol
ISP	Internet Service Provider
ITSP	Internet Telephony Service Provider
ITSPA	Internet Telephony Service Providers' Association
LAN	Local Area Network
OTT	Over The Top
NAT	Network Address Translation
RFC	Request For Comment (IETF Standards)
RTP	Real-time Transport Protocol
RTSP	Real Time Streaming Protocol
SDP	Session Description Protocol
SIP	Session Initiation Protocol
UA	User Agent
VoIP	Voice over IP
WAN	Wide Area Network

4 Application Layer Gateways (ALG)

4.1 General

An Application Level Gateway acts as an intermediate system between the Internet and the application server that understands the relevant application protocol. It allows customised NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer control/data protocols such as FTP, SIP, RTSP, etc.

4.2 Associated Router functions

4.2.1 Firewall

A firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules. A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted. Firewalls can be either hardware or software but the ideal firewall configuration will consist of both.

4.2.2 NAT

Network Address Translation (NAT) is a method of remapping one IP address space into another by modifying network address information in IP headers while they are in transit across a router.

NAT was originally used for ease of rerouting traffic in IP networks without readdressing every host. It has become a popular and essential tool in conserving global address space allocations due to IPv4 address exhaustion by sharing one Internet-routable or WAN (Wide Area Network) IP address with many LAN (Local Area Network) side devices.

5 SIP ALG

5.1 General

Despite SIP ALG being intended to assist with such scenarios as a network of SIP End Points on a LAN behind a router, it is implemented inconsistently and causes poor user experience.

It has been observed that implementations of SIP ALG often modify SIP packets in ways which gives rise to service issues, such as SIP endpoints not registering, one way media and incoming calls failing.

SIP ALGs were initially created to help solve the problem of SIP traversing firewalls and in particular NAT environments. The SIP ALG inspects the SIP headers and SDP message bodies as they pass through the router and may alter the data, in particular rewriting references to the internal IP of the SIP device and replacing it with the public IP address of the Internet connection. For the majority of routers this is the basic and sole use for a SIP ALG.

With SIP ALG disabled the SIP traffic is unaltered. The NAT functionality of the router will only manipulate the layer 3 addressing, with no alteration of the SIP headers. The problem of internal IP addresses in the SIP headers is then delegated to the external SIP server and the majority of ITSPs prefer this since this is a relatively straightforward task for SIP endpoints.

5.2 Problems arising using SIP ALG

Service problems caused by SIP ALG are not always apparent on initial implementation but may manifest over the lifetime of the service.

5.2.1 Initial implementation

With even minor differences in implementation, a SIP ALG can affect the correct operation of SIP phones. Some SIP ALGs have an inability to deal with anything other than basic SIP traffic.

For example:

- The inability to route SIP signalling and media correctly to multiple SIP Phones or SIP accounts
- The disruption caused by the interaction of SIP ALG and NAT mapping

5.2.2 Service development

A VoIP service traversing a router with the SIP ALG enabled can appear to work with limited testing of a single phone but upon inspection or greater use / testing the following problems may become apparent:

- Incoming calls do not ring the correct phone
- One way audio may be encountered
- Transferring of calls does not work
- Message Waiting indicators do not work

5.2.3 Future/intermittent service failures

The following issues are not always apparent at the initial deployment of the SIP service -

- Phones start to randomly fail re-registration with SIP servers
- New phones fail to register to SIP servers

5.3 Scenarios that may require SIP ALG to be enabled

Some router and networking manufacturers use SIP ALGs to deliver advanced features. Where a router manufacturer is also a provider of SIP phones and servers there are often customisations that are implemented in SIP ALGs. For example, a SIP phone might register with an external SIP server in another location. If the router detects the WAN or Internet has failed the SIP traffic is rerouted by the SIP ALG to an Internal SIP server that can provide basic extension dial or alternative routeing of calls to emergency services.

SIP ALG can be used to alter the path taken for SIP media traffic to force the call to stay on the internal network for two devices known to be on the same subnet which may prevent inefficient routeing of phone call traffic out to an external SIP server and back in again, reducing bandwidth and latency.

5.4 SIP ALG – Recommendations for management

Given that the vast majority of SIP ALG implementations are not needed by the Service Provider, we recommend the following in regard to SIP ALG operation.

- SIP ALGs should be turned off for Hosted voice services
- SIP ALGs should be able to be turned off and on by end users with a simple process as part of the normal administration of the equipment
- Configuration status display should clearly indicate that a SIP ALG is either off or on

5.4 Guidance on the impact on IPv6

IPv6 offers many benefits including more efficient packet routing, processing, network configuration and the elimination of the need for Network Address Translation (NAT).

Therefore, ALGs (including SIP ALG) which are deployed to assist NAT will not be required in a full IPv6 environment. However, during the transition from IPv4 to IPv6, NAT will continue to be necessary and ALGs (including SIP ALG) will continue to be deployed.

In an IPv6 implementation, ALGs may still be required for functions other than NAT, e.g. firewall functionality, traffic blocking etc.

6 Guidance for the implementation of SIP ALG

Due to the impact of SIP ALG on some services, e.g. hosted voice, careful consideration must be given as to whether SIP ALG is required or deployed in individual cases.

Most CPs are working towards supplying CPE “routers” with the default setting of SIP ALG disabled. In general having a SIP ALG function enabled (within the CPE) does not work with hosted and OTT SIP based services.

Given that the vast majority of SIP ALG implementations are not needed by the Service Provider, we recommend the following in regard to SIP ALG operation.

- SIP ALGs should be disabled by default
- SIP ALGs should be easily configurable (i.e. to be disabled/enabled) by end users as part of the normal administration of the equipment
- Configuration status display should clearly indicate that a SIP ALG is either disabled or enabled

Annex A.1 ITSPA SIP ALG survey

The following information is a summary of the results from a 2016 survey commissioned by ITSPA and sent to its members.

The following questions were sent to ITSPA member organisations and the results of their member replies are included below.

The question responses permitted were Yes/No/ Don't know.
The tables indicate the percentage respondents choosing a specific response. Beneath the percentage is the actual number of responses.

A.1.1 Are you aware of the benefits provided by SIP ALG?

Answer Choices	Responses
Yes	**70.00%** 28
No	**25.00%** 10
Don't know	**5.00%** 2
Total	40

A.1.2 Are you aware of any problems SIP ALG causes?

Answer Choices	Responses
Yes	**92.50%** 37
No	**2.50%** 1
Don't know	**5.00%** 2
Total	40

A.1.3 Is SIP ALG needed for delivering your service?

Answer Choices	Responses
Yes	**2.50%** 1
No	**90.00%** 36
Don't know	**7.50%** 3
Total	40

A.1.4 Is any ALG needed for delivering your service?

Answer Choices	Responses
Yes	2.50% 1
No	85.00% 34
Don't know	12.50% 5
Total	40

A.1.5 Should it be possible to enable/disable the SIP ALG from the CPE admin GUI?

Answer Choices	Responses
Yes	92.50% 37
No	0.00% 0
Don't know	7.50% 3
Total	40

A.1.6 If SIP ALG is included as a feature on a broadband router (or CPE) do you believe it should be disabled by default?

Answer Choices	Responses
Yes	87.50% 35
No	2.50% 1
Don't know	10.00% 4
Total	40

History

Document history		
Version	Date	Milestone
1.1.1	March 2017	Initial publication