3GPP TR 33.830 V0.4.1 (2013-09)

Technical Report

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Study on firewall traversal (Stage 2)
(Release 12)

Keywords
security, firewall, tunnelling, SIP, authentication

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

Introduction

This clause is optional. If it exists, it is always the second unnumbered clause.

1 Scope

The present document:

a) studies requirements and scenarios for traversal of IMS services over IMS-unaware firewalls (Non-IMS Aware Firewall - NIMSFW); and

b) studies mechanisms (based on both secure and non-secure tunnels), which can be used for traversal of IMS services over IMS-unaware firewalls.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[2] 3GPP TS 41.101: "Technical Specifications and Technical Reports for a GERAN-based 3GPP system".

[3] 3GPP TS 33.401: "3GPP System Architecture Evolution (SAE); Security architecture".

[5] 3GPP TS 22.228: ""Service Requirements for Internet Protocol (IP) multimedia core network subsystem (IMS); Stage 1".

[6] 3GPP TS 43.318: "Generic Access Network (GAN); Stage 2

[7] 3GPP TS 24.229: "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[8] 3GPP TS 33.203: "3G security; Access security for IP-based services".

[9] 3GPP TS 23.228: "IP Multimedia Subsystem (IMS); Stage 2".

[10] 3GPP TS 44.318: "Generic Access Network (GAN); Mobile GAN interface layer 3 specification".

[11] 3GPP TS 23.234: "3GPP system to Wireless Local Area Network (WLAN) interworking; System description".

[12] 3GPP TS 24.237: "IP Multimedia (IM) Core Network (CN) subsystem IP Multimedia Subsystem (IMS) service continuity; Stage 3".

[13] 3GPP TS 23.402: "Architecture enhancements for non-3GPP accesses".

[14] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TR 21.905 [1] and the following apply.
A term defined in the present document takes precedence over the definition of the same term, if any, in TR 21.905 [1].

Definition format (Normal)

<defined term>: *<definition>.*

example: text used to clarify abstract rules by applying them literally.

Non-IMS Aware Firewall (NIMSFW): type of firewall which is IMS-unaware and will block IMS services.

3.2 Symbols

For the purposes of the present document, the following symbols apply:

Symbol format (EW)

<symbol> <Explanation>

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in TR 21.905 [1] and the following apply.
An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in TR 21.905 [1].

DPI	Deep Packet Inspection
FIRE	FIREwall traversal
FQDN	Fully Qualified Domain Name
FW	Firewall
IANA	
IMS	
NAT	Network Address Translation
NIMSFW	Non-IMS Aware Firewall
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
P-CSCF	Proxy Call Session Control Function
RTCP	
RTP	
SIP	
SMURF	Service and Media Reachability for Users over Restrictive Firewalls
TCP	
TDF	Traffic Detection Function
UDP	
VoIP	

4 Background

Editor's notes: This clause gives an over view on various kinds of Firewalls which will allow IMS traffic to go through and Firewalls which will block IMS traffic (NIMSFW).

4.1 Overview of IMS protocols

Table 4.1 gives a summary of the current IMS protocols, transport protocols, and default ports. This clarifies the current protocol situation in IMS and make sure that every IMS protocol is considered in the solution assessment.

Transport protocol: SIP is normally sent on UDP. In fact this is just one of several options, and because of the increasing SIP messages sizes, it is now more common to send SIP over TCP. New VoIP clients have actually begun dropping support of SIP over UDP.

Default port number: It should be noted that protocols are always sent on their default port numbers. In fact, the default port number is just a default and, with a few exceptions, protocols are allowed to use any port number. While SIP is often sent on the default port numbers, it is both allowed and common to use other ports. For protocols like RTP and RTCP, the situation is the opposite and the default port numbers are almost never used (except by accident).

Table 4.1: Overview of IMS protocols

Protocol	Transport Protocol	Default port	Comment
SIP	UDP	5060	
	TCP	5060	SIP over TCP is the de facto standard today due to increasing SIP message sizes.
	TLS/DTLS	5061	The default transport for TLS is TCP. The default transport for DTLS is UDP.
RTP	UDP	5004	Often even port. Default port is seldom used.
	TCP	5004	TCP is not commonly used.
RTCP	UDP	5005	Often RTP port + 1. Default port is seldom used.
	TCP	5005	TCP is not commonly used.
MSRP	TCP	2855	This is the suggested port for MSRP and is seldom used
RTSP	TCP	554	
BFCP	TCP	5070	
	TLS	5070	New IETF recommendations are to use same port for TLS. The default transport for TLS is TCP.
HTTP	TCP	80	Port is often open in firewalls.
	TLS	443	Port is often open in firewalls. The default transport for TLS is TCP.
DNS	TCP/UDP	53	

NOTE: Table 4.1 gives a subset of the default ports. A complete list of IANA assigned ports could be found at: http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml.

4.2 Relationship between FIRE and SMURF

FIRE: The study on Firewall traversal (FS_FIRE) in 3GPP WG SA3 means to achieve traversal of IMS services over IMS-unaware firewalls. The scope has been expanded to also cover the needs of firewall owner:

- Only IMS services;
- Both mobile and fixed IMS UEs.

SMURF: Stage 1 on Service and Media Reachability for Users over Restrictive Firewalls (SMURFs) in 3GPP WG SA1 means to achieve UE access to PLMN IP-based services over restrictive firewalls in non-3GPP accesses. The scope has been expanded to also cover the needs of firewall owner:

- All PLMN IP-based services;
- Only mobile UEs.

The worst case scenario in FS_FIRE and SMURF is an application aware/DPI firewall restricted to TCP on port 80 or 443 combined with a web proxy. To traverse restrictive firewalls both solutions needs to use TCP (set up with HTTP CONNECT), use port 80 or 443, and look like HTTP/HTTPS.

The high level coverage and overlap of FS_FIRE and SMURF is shown in Figure 4.2 .

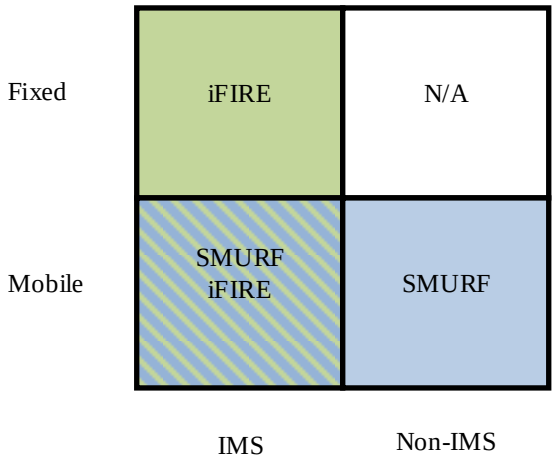


Figure 4.2: FS_FIRE and SMURF overview and overlap

While an FS_FIRE solution may or may not fulfill the SMURF requirements, a solution fulfilling the SMURF requirements also fulfills the FS_FIRE requirements (at least for 3GPP UEs).

The possible outcomes from the FS_FIRE/SMURF work items are:

- FS_FIRE and SMURF are specified independently and therefore overlap when it comes to IMS services for 3GPP UEs.
- The SMURF solution is used by 3GPP UEs to access all services (both IMS and non-IMS). FS_FIRE is focused to solve the firewall traversal problem for fixed IMS UEs accessing IMS services.

From the analysis it is clear that the work items are largely overlapping. In general overlapping solutions should be avoided as this increases both the work effort and the complexity. FS_FIRE and SMURF should therefore be studied together. However, it should be studied further whether an FS_FIRE solution would allow for a simpler realization than a SMURF solution, or could be a profile of a SMURF solution. As an example, it should be studied further whether

FS_FIRE could benefit from IMS security, making an extra layer of client authentication as part of the FW traversal mechanism unnecessary. As another example, double protection for IMS media could be avoided in FS_FIRE as IMS media protection is initiated by the client and the client would be aware of the use of FS_FIRE. For general applications, there is no equivalent to IMS security, and no corresponding statements on general application security could be made.

Furthermore, IMS represents a well-established and elaborate architecture, which has no equivalent for general applications. Therefore, any SMURF solution should be evaluated with respect to its suitability for IMS and FS_FIRE.

4.3 NAT/FW types

This clause provides background on various kinds of NATs and Firewalls (FW) devices and the restrictions those devices could impose on IMS traffic.

The NAT traversal mechanisms specified in 3GPP TS 24.229 [7] allows traversal of IMS traffic through certain kind of NAT/FW devices. The following clause gives the list of those kinds of NAT/FW devices.

1. **Full-cone NAT**, also known as *one-to-one NAT*
   - Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
   - *Any external host* can send packets to iAddr:iPort by sending packets to eAddr:ePort.

2. **(Address) restricted cone NAT**
   - Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
   - An external host (*hAddr:any*) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:*any*. "Any" means the port number doesn't matter.

3. **Port-restricted cone NAT**
   - Like an address restricted cone NAT, but the restriction includes port numbers.
   - Once an internal address (iAddr:iPort) is mapped to an external address (eAddr:ePort), any packets from iAddr:iPort will be sent through eAddr:ePort.
   - An external host (hAddr:hPort) can send packets to iAddr:iPort by sending packets to eAddr:ePort only if iAddr:iPort has previously sent a packet to hAddr:hPort.

4. **Symmetric NAT**
   - Requests from internal IP address and port pairs to different external IP address and port pairs are mapped to the external NAT address on a unique port. This also applies to all requests from the same host to different destinations.
   - Only an external host that receives a packet from an internal host can send a packet back.

The following clause gives the list of NIMSFW related to the use cases, where further clarifications of how existing solutions can solve the firewall access should be studied or whether further work needs to be done should be analysed.

5. **Port Restricted NAT/FW**
   - Requests to and from internal IP address and port pairs could only be to/from specific ports. In other words only specific application ports are opened such as port 80 for HTTP traffic and port 443, for HTTPS traffic. In the most "secure" case this would be only port 443.

6. **TCP** Restricted **NAT/FW**
   - Requests to and from internal IP address and port pairs must be TCP. In other words Protocol field in IP header must indicate that this is TCP packet. (i.e., no UDP).

7. **Specific Port TCP Restricted NAT/FW**
   - This is a combination of Port Restricted NAT and TCP Restricted NAT
   - An example would be a NAT device that allows TCP only communication on port 443 (https)

8. **Firewall with HTTP Proxy**

When a firewall has a built in explicit HTTP proxy as shown in Figure 4.3-1, the firewall does not allow the IMS traffic through go through unless the IMS application establishes a proxy TCP connection through the HTTP proxy using the HTTP CONNECT method (RFC 2616).
Figure 4.3-2 gives an overview of HTTP CONNECT handshake.

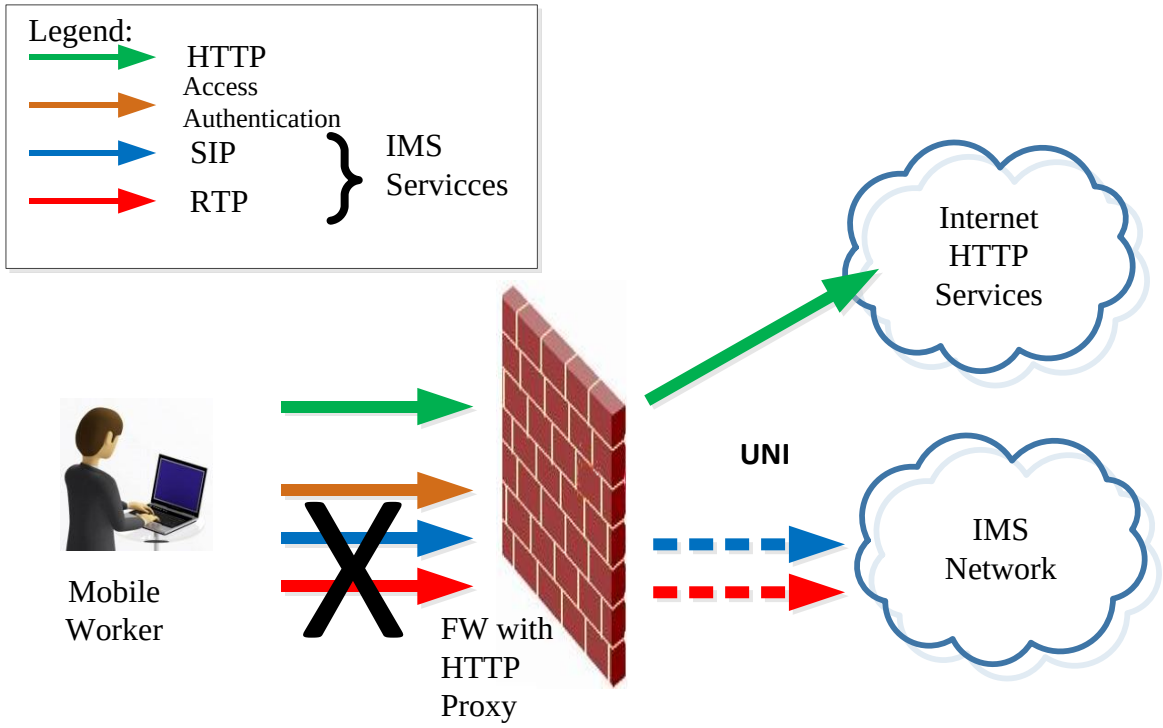


Figure 4.3-1: SIP IMS services blocking by "FW with HTTP Proxy"

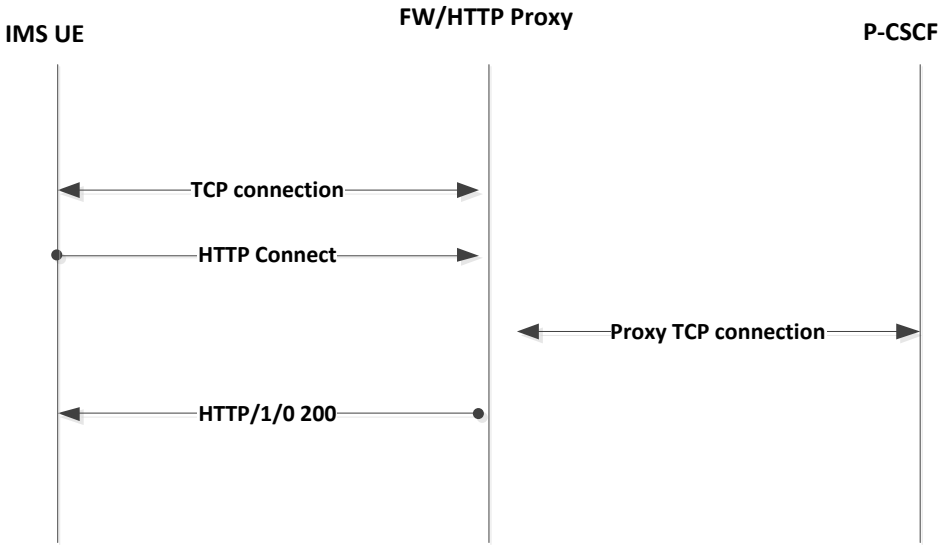


Figure 4.3-2: Establishing Proxy TCP connection through HTTP Proxy using HTTP CONNECT method

9. Firewall with Deep Packet Inspection (DPI) capability and Application Awareness

Many of the enterprise firewalls have DPI capabilities and are application aware. These kinds of firewalls can block IMS traffic by performing DPI on IMS traffic (for example, SIP packets going to default UDP/TCP port of 5060/5061 can be blocked by doing a DPI on the IP/UDP packet). Further, if the firewall is application aware, IMS traffic could be blocked by these firewalls doing application level inspection of the packet (for example, firewall device can look for SIP requests INVITE or REGISTER and then block the traffic).

4.4 Premises placed firewall and NAT traversal

Firewalls may be placed within a premises and within the administrative domain (enterprise/residential) of that premises. The firewall operator may be a residential consumer or enterprise, or the consumer or enterprise may have delegated such to a service provider or operator which may or may not be distinct from the operator desiring to extend IMS services over the consumer's or enterprise's network.

NAT traversal as a function either with or without a firewall is to be considered.

A premises firewall operator may desire or require the following within its administrative domain:

- To restrict all IMS traffic for access or to permit all IMS traffic that traverses its network border;
- To allow per user or device policy decisions to allow or deny IMS traffic that traverses its network border;
- To allow for the detection of IMS traffic within its administrative domain to effect policy decisions and policy enforcement.

Premises firewall operators may need such restrictive policies for a variety of reasons, including but not limited to:

- To protect its network from services it may view as unsafe or unauthorized;
- To prevent or limit consumption of network resources from unauthorized applications;
- To prevent or limit it or its agents from violating commercial terms of service from its internet service provider that may not permit access save for the purpose of email, browsing, or file transfer.

4.5 Network placed firewall and NAT traversal

Firewalls may be placed at various places within the network to effect policy (including policies related to providing services to residential and/or enterprise consumers but additionally policies related to the operation of its own network). The effect of a network placed firewall must be considered.

NAT traversal as a function either with or without a firewall is to be considered.

In this case, the firewall provider is a provider of network services and may additionally be a provider of terrestrial or mobile Internet or IP or broadband access directly to residential consumers or to enterprises.
The firewall provider may also provide transport between various consumer or enterprise networks and other networks.
The firewall provider may also host firewall and/or policy enforcement services within the network on behalf of residential consumer or enterprises it provides services to (whether as access, transport, firewall hosting, and/or network based policy enforcement).

A network firewall provider that provides services to residential consumer or enterprises may be viewed to have the same requirements as the premises firewall operator as the requirements of the premises firewall operator pass to the network firewall operator.

Network firewall operators as internet service providers or providers of mobile access have special considerations similar to that of premises firewall operator.

A network firewall operator may desire or require the following within its administrative domain:

- To restrict all IMS traffic for access or to permit all IMS traffic that traverses its network border.
- To allow per subscriber or device policy decisions to allow or deny IMS traffic that traverses its network border.
- To allow for the detection of IMS traffic within its administrative domain to effect policy decisions and policy enforcement.

Additionally network firewall operators may need such restrictive policies for a variety of reasons, including but not limited to:

- To enforce its network policies and/or business agreements. A mobile operator that provides access may or may not welcome the offering of IMS services of another operator without a business arrangement in place.
- To effect reasonable network management for whatever reason, such as to IMS services offered "over the top" (e.g., as a service via SGi/Gi on the Internet or to some IP administrative domain, e.g., an enterprise providing its own IMS services).
- To prevent or reduce its consumer or enterprise subscribers from using IMS services that violate the terms of service they have agreed to, such as limiting Internet access to browsing, file transfer, and email as may be commonly found in many commercial terms of service.

4.6 Premises and network placed firewall and NAT traversal

Both premises and network based firewalls may exist simultaneously.
The firewall traversal methods must consider the simultaneous operation of both premises and network based firewalls.

NAT traversal as a function either with or without a firewall is to be considered including the presence of multiple NATs.

4.7 Premises/network policy enforcement

Firewalls are a specific embodiment of a Policy and Charging Enforcement Function (PCEF) but other embodiments exist, such as HTTP proxies or DPI-aware PCEF distinct from firewalls.

While the general case of bypassing the firewall and policy enforcement may be thought of benefit to an IMS service provider, it may be at the expense of the firewall operator (whether residential, enterprise, terrestrial or broadband access provider including mobile Internet or IP network access, and/or transport provider) who may wish to install firewalls, proxies, or other PCEF to enforce its policies.

The following may be needs in addition to firewall traversal:

- Consideration for IMS traffic to pass through PCEF other that firewalls;
- Consideration for IMS traffic to pass through HTTP proxies;
- Consideration of the policy enforcement and policy discrimination needs of the firewall operator;
- Consideration for premises based policy enforcement and discrimination as well as network-based policy enforcement and discrimination.

4.8 Mechanisms to enable blocking of IMS traffic

4.8.1 Implicit markers

An implicit marker is a marker that already exists in the packet for other reasons than making the firewall aware of IMS traffic.

One implicit marker that exists in every packet in every solution is the IP address and port number, or FQDN belonging to a server controlled by the IMS operator. If the firewall has knowledge of the IP address or range of IP addresses, it is clear the firewall can easily both detect and block the traffic if needed.

While it may not be realistic for a FW operator to know the IP address of every server of every IMS operator in the world, it might be realistic to assume that the firewall owner may have knowledge of the national servers used by IMS operators used for firewall traversal. The possibility of this can be increased by recommending IMS operators to use a similar way of marking the entry P-CSCF's to the network that are to be used (e.g. P-CSCF.operator.com).

Other implicit markers than IP addresses differ from solution to solution and should be discussed in respective solution.

Implicit markers has the big benefit of not adding any overhead, they are also unlikely to cause compatibility problems are divert from IETF standards and common protocols implementations

4.8.2 Explicit markers

An explicit marker is a marker that is put into the packet for the single reason of making the firewall aware of IMS traffic.

The benefits with an explicit market is that it is easy to detect, does not give any false classifications and (depending on where it is placed) should require little processing in the firewall. The same marker can also be reused in several different mechanisms.

Disadvantages are that an explicit marker adds overhead, may cause compatibility problems with older releases or older deployments, and may not be compliant with IETF standards,

An explicit marker can be inserted in several places, e.g. HTTP CONNECT request, TLS/IKE handshake, or in the security protocol.

Inserting the marker in the security protocol adds significant overhand and is not standard compliant, inserting a marker in the TLS/IKE handshake might not be standard compliant and may require extensions to standard implementations to the protocols.

By placing the explicit marker as a header in the HTTP CONNECT request most or all of these issues disappear.
HTTP is designed to allow the insertion of registered or unregistered headers.
No node or server should have problems with a HTTP header.

There are several existing registered and non-registered (X-) headers that could be used to mark IMS traffic.
Alternatively a new registered and non-registered header could be used. Below some examples are listed:

```
CONNECT server.example.com:80 HTTP/1.1

Host: server.example.com:80

From: john.doe@example.com

Pragma: Firewall Traversal

User-Agent: 3GPP-IMS-FS_FIRE
```

```
Warning: IMS traffic

X-Powered-By: 3GPP SA3 FS_FIRE
```

As there is a requirement to traverse HTTP proxies, all solutions must use HTTP CONNECT.
In this approach, in the absence of HTTP Proxy in the networks, the HTTP_CONNECT is not consumed by the firewall and hence in this scenario the core network element should be able to handle/consume this message.

4.8.3 Traffic flow analysis

Traffic flow analysis means that the NIMSFW detects IMS traffic based on packet sizes, frequencies and timing. Using traffic flow analysis is technically feasible but has some disadvantages for the firewall operator. It is more resource demanding that other techniques and as the mechanism is probabilistic and not deterministic it may give some false classifications. The benefits are that the solution does not add overhead, does not impact UE and operator network and does not cause any compatibility problems.

How traffic flow analysis in done is implementation specific to each firewall vendor. To enable the possibility to do traffic flow analysis the use of traffic flow confidentiality mechanisms (for the purpose of hindering detection of) could be forbidden.

4.8.4 Conclusions and proposed mechanism

Based on the analysis above the following mechanisms are recommended:

- The UE should include a standardized header in the HTTP CONNECT request identifying that the connection is meant to be used for IMS traffic. Details of the HTTP header are left for stage 3.
- IMS operators are recommended to publish the FQDNs of servers used for firewall traversal. How this is published is out of scope, but the information should be easy for firewall operators to find and use.

NOTE: One of the FS_FIRE use cases is for enterprise networks that use off-the-shelf firewalls and/or lack skilled IT administrators. It will, by this assumption, not be possible to take advantage of the proposed method in such networks due to the impossibility to make the required changes to the firewall. And yet, such enterprise networks may have a policy to block IMS traffic. This policy would then be overriden by the FS_FIRE mechanism.

Editor's note: The use cases and requirements in clauses 4.1-4.4 are for further study and inclusion pending SA1 input.

4.9 Problems with using TCP

It has been agreed that to traverse restrictive firewalls, the solution needs to use TCP (set up with HTTP CONNECT), use port 80 or 443, and look like HTTP/HTTPS. TCP provides reliable ordered delivery of a stream of octets.
Due to network congestion, traffic load balancing, or other unpredictable network behaviour, IP packets can be lost, duplicated, or delivered out of order. When this happens, the TCP stack has to wait for the out-of-order packets or retransmission of lost packets. This can lead to relatively long delays (potentially in the order of seconds).
These problems are enhanced by the fact that the access where the firewall traversal mechanism is used cannot be assumed to fulfil any quality of service requirements.

Using a reliable and ordered protocol like TCP instead of UDP to transfer real-time media is especially problematic as delays are directly noticeable and may be unacceptable for the subscriber. If several different sessions are transported over the same TCP connection the problem are even worse as a single out-of-order or lost packet in one session leads to delays in all of the sessions, a single out-of-order or lost packet in the control plane or any of the media sessions leads to delays in both the control plane and all of the media sessions. An out-of-order or lost packet in the control plane negatively effects the media plane and vice versa.

Editor's Note: Solutions should show how they take care of the problems mentioned above.

5 Use cases

5.1 Use cases relating to IMS service access

The service requirement for IMS firewall traversal is specified in 3GPP TS 22.228 [5] and reads as follows:

> *"IM CN should provide support for the users to access IM CN through a Firewall (FW) with configuration restrictions (e.g. only HTTP allowed, port range limitation) deployed outside operators' domain."*

This clause explores the use cases relating to this service requirement to help derive and motivate functional requirements and security requirements on potential solutions, which are then documented in a later clause of the present document.

As seen from clause 4, there are multiple types of firewalls that may exist in IP access networks and that may be configured to block one or more of the IMS protocols when they are carried natively over IP (e.g. SIP, RTP, MSRP, RTSP, ….).
In the case that these firewalls are deployed outside the IMS operators' domain of control, there are limited possibilities for the IMS operator to request to open the necessary ports needed to allow IMS services to be transported natively over the firewall. Consequently, it is necessary to investigate whether acceptable alternative solutions can be found which provide reachability to the IMS core without requiring changes to be made in the firewall.

Whilst firewalls vary considerably with respect to the protocols that are allowed or blocked, an almost universal characteristic is that outbound web traffic (HTTP/HTTPS) is allowed. For this reason, any solution to provide IMS core reachability across the widest range of firewalls would most naturally tunnel the IMS protocols inside something that looks like HTTP or HTTPS to the firewall. A further restriction made by some firewalls is that all outbound web traffic must be routed through an HTTP proxy and so a solution that accommodates this would also improve reachability towards the IMS core.

3GPP specifications exist for tunnelling IMS protocols over IPsec (e.g. TS 43.318, TS 33.234 and TS 33.402). However, whilst these solutions could be used to traverse some types of firewalls, they would not work over firewalls which block IPsec and would very likely provide a lower level of reachability when compared to a solution based on something that looks like HTTP/HTTPS to the firewall.

Whilst tunnelling IMS protocols over IPsec or something that looks like HTTP/HTTPS to "traverse" a fire wall does not technically break any firewall rules, one may argue that it serves to make those rules less effective in blocking IMS if that is indeed the intention of the firewall operator. However, in many cases a firewall that is blocking native IMS protocols may not be intending to explicitly block IMS or other IP communication services. Instead the network may be applying a simple "deny by default" policy whereby IMS protocols would be explicitly blocked unless there is an explicit request to unblock them. Furthermore, multiple protocols and communication services are routinely tunnelled over HTTP/HTTPS by applications so it is naive on the part of any firewall operator to assume that blocking everything but HTTP/HTTPS would guarantee that only "conventional" web traffic can traverse its network.

For firewall operators that do intentionally want to block IMS or other IP communication services, it is important to recognize that there would still exist methods to block those services even if HTTP/HTTPS tunnelling is used.
For example, firewalls may employ traffic analysis or block IP address ranges of servers that provide the IMS or IP communication service. Alternatively, access networks may employ end point security to control which applications connecting devices can use on the network.

Editor's Note: IP addresses of IMS or IP communication services may not be known to firewall operators or may be dynamic. It is ffs whether this possibility should be included as an example in the TR.

Client authentication can also guard against Denial of Service (DoS) attacks on the network infrastructure used to support firewall traversal.

Editor's Note: The scope of such DoS attacks and, if required, alternative ways to mitigate them are ffs

An alternative solution to tunnelling IMS over HTTP/HTTPS would be for the IP access network to open the necessary ports to allow IMS communication. However, this may actually expose the IP access networks to more risks than in the case where only outbound HTTP/HTTPS traffic is allowed and the client devices use an HTTP/HTTPS tunnelling

mechanism. For example, opening SIP ports may expose the IP access network's internal SIP and RTP services to unauthorised access and attack from external networks. So it is incorrect to conclude that introducing HTTP/HTTPS tunnelling undermines the value of an access network firewall that only allows HTTP/HTTPS.

5.2 Use cases based on access types

Editor's note: The following use cases are out of scope for FS_FIRE (from the perspective of changing FW traversal for those existing mechanisms and are in scope from the perspective of IP interface selection) and could be in the scope for SMURF:

- Untrusted non-3GPP access (3GPP 23.402 [13])
- GAN Access (3GPP 43.318/3GPP 44.318)
- 3GPP access (PS access via GPRS, EDGE, UMTS, HSPA, LTE, LTE-A and WLAN)

5.2.1 WLAN Direct IP Access

Figure 5.2.1 shows WLAN network model (3GPP TS 23.234 [11]). According to 3GPP TS 23.234, the WLAN Direct IP Access service allows authorized subscribers to access local IP networks such as the Internet or Intranet directly from the WLAN AN. The interface to the 3GPP AAA server is only for the signalling interface and the user traffic from the WLAN UE goes directly to the Intranet/Internet.

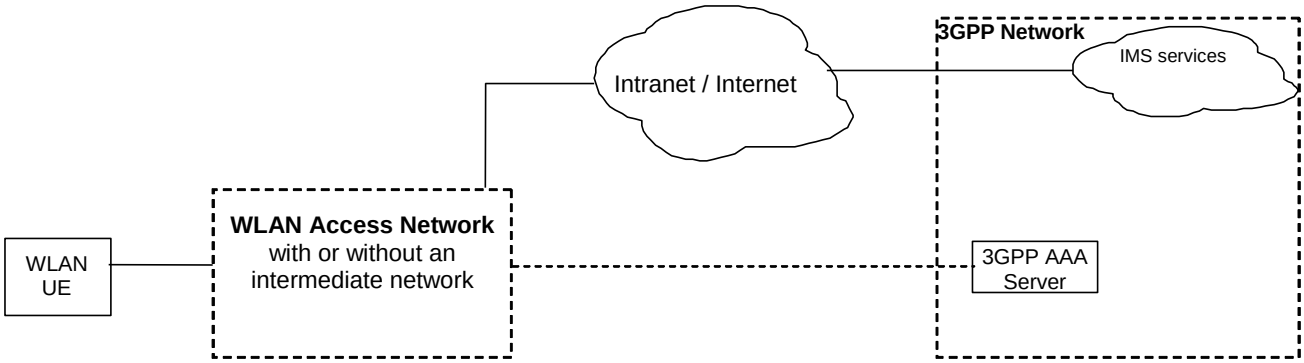


Figure 5.2.1: Simplified WLAN network model

If IMS services run over WLAN Direct IP Access network and if there are NIMSFW in the WLAN Direct IP Access network, the IMS services could be blocked by the NIMSFW thus preventing the operator from running the IMS services.

NOTE: The IMS Services and the 3GPP AAA server could potentially be operated by different operators.

5.2.2 Trusted non-3GPP access

According to 3GPP TS 23.402 [13], whether a non-3GPP IP access network is Trusted or Untrusted is not a characteristic of the access network. In non-roaming scenario it is the HPLMN's operator decision if a non-3GPP IP access network is used as Trusted or Untrusted non-3GPP access network. In roaming scenario, the HSS/3GPP AAA Server in HPLMN makes the final decision of whether a non-3GPP IP access network is used as Trusted or Untrusted non-3GPP access network.

Figure 5.2.2 shows non-roaming architecture with EPS using S5, S2a and S2b. S2a interface for Trusted non-3GPP IP Access supporting PMIPv6 [RFC 5213] and Client Mobile IPv4 Foreign Agent (FA) mode based on RFC 3344 and RFC 3024.

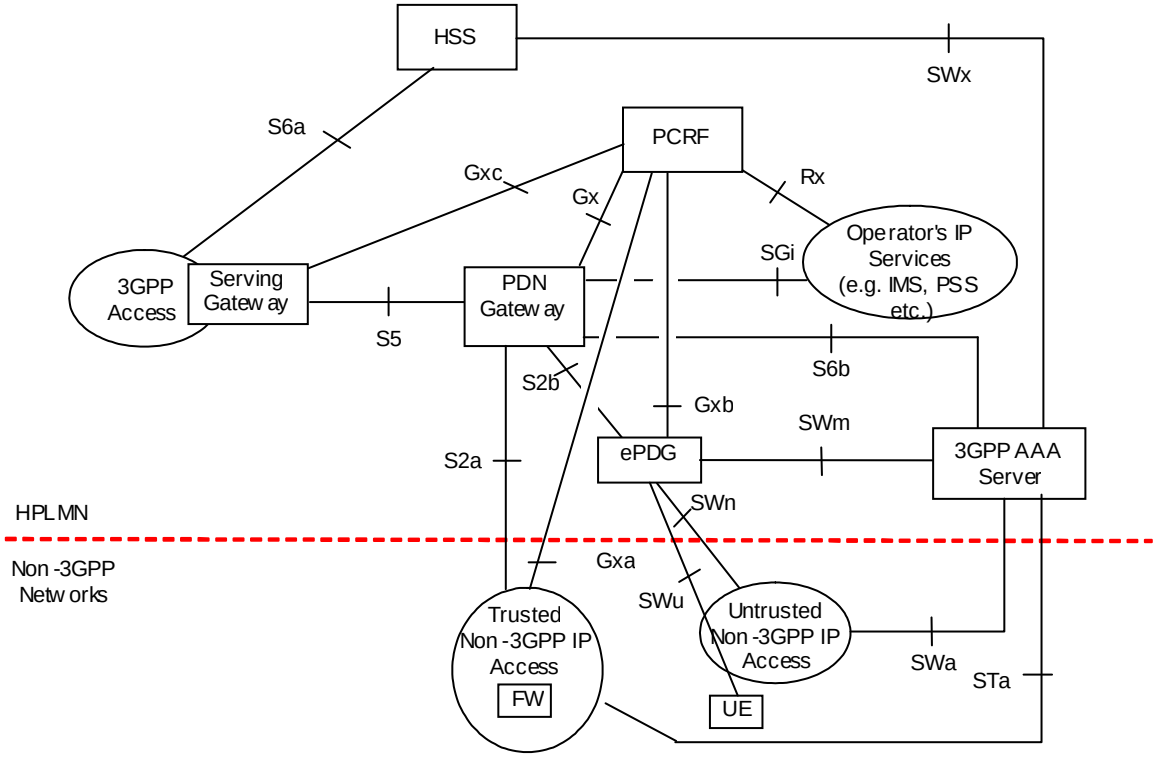


Figure 5.2.2: Non-roaming architecture within EPS using S5, S2a,S2b

Based on RFC 3344, the packets from the MN to the CN are carried as IP packets destined to the CN.
If RFC 3024 mechanism is used, the packets destined to the CN are tunnelled to the FA using RFC 2003 datagrams.
So, if there is NIMSFW present in the Trusted non-3GPP IP access network while using RFC3344 or RFC 3024 based mechanism, the IMS traffic from the UE could be blocked by the NIMSFW thus making it not possible to run IMS services.
Similarly, NIMSFW could also block IMS traffic while using PMIPv6 based on RFC 5213.

NOTE: 3GPP TS 23.402 [13] has many different architecture scenarios for both roaming and non-roaming scenarios where presence of the NIMSFW could block the IMS traffic.
See 3GPP TS 23.402 clause 4.2 (Architecture Reference Model) to get more information on these possible architectures.

5.2.3 TISPAN & Generic IP Access

The ETSI Technical Body "Telecommunication and Internet converged Services and Protocols for Advanced Networking" (TISPAN) adopts the 3GPP IMS architecture for SIP based applications.
ETSI TR 180 001 v1.1.1, states that TISPAN architecture is required to support access networks of diverse technologies and capabilities. Example of "Access Network" given in the above ETSI TR includes xDSL, optical access, Gigabit Ethernet, cable networks, 3GPP or 3GPP2 PS domain and other wireless access network types.

ETSI TR 187 008 v1.1.1 is the NAT traversal feasibility study report for TISPAN architecture and analyzes various NAT traversal mechanisms and limitation with those mechanisms in running IMS services in the TISPAN architecture. Given the wide range of access networks supported by the TISPAN architecture, one could have NIMSFW in the path between the UE and the P-CSCF (Gm interface) which could block IMS services thus limiting the use of TISPAN architecture for running IMS services.

Editor's Note: It should be ffs that how the FS_FIRE solutions would solve the firewall traversal issue when signalling and media uses different IP addresses and traverse through different paths, e.g., P-CSCF and IMS-AGW may be deployed on different devices.

6 Requirements

Editor's notes: This clause contains requirements resulting from this study.

The following requirements are derived from the use cases in clause 5.

6.1 Functional requirements

The solution **shall**:

1. Support traversal of IMS services across firewalls which only allow outbound HTTP/HTTPS traffic
2. Support traversal of IMS services across firewalls which require outbound traffic to be routed through an HTTP proxy
3. For traversal not require changes to the Firewall
4. Minimize changes to the UE
5. Support all the existing IMS protocols (SIP, RTP, MSRP, RTSP, HTTP…..)
6. Support detection of IMS restrictive firewalls
7. Be transparent to the existing IMS core Editor's note: The trade-off between transparency and efficiency should be studied further for requirement 7.
8. Be compatible with existing IMS architecture, particularly the separation between the user and control plane
9. Allow other 3GPP Firewall traversal mechanism to exist in parallel
10. Allow selective invocation of firewall traversal and/or security functionality introduced through the proposed solutions when needed
11. Not break the IMS threat model
12. iFire shall not preclude the operation of non-3GPP IP access methods defined in 23.402 [13], GAN/UMA defined in 3GPP TS 43.318 [6], or 3GPP system to Wireless Local Area Network (WLAN) interworking defined in 3GPP TS 23.234 [11]
13. The methods for iFire shall consider whether an existing IP access mechanism, such as non-3GPP IP access, GAN/UMA, or 3GPP system to Wireless Local Area Network (WLAN) interworking will traverse a firewall
14. Support all kinds of IMS UE, both fixed and mobile
15. Support the firewall operator's need to make local policy decisions on traffic that is intended to traverse its firewall(s) and policy enforcement function(s).
16. Support integration with and provide access through policy architecture elements and functions including PCRF, TDF, and PCEF placed with or separately from firewall(s).
17. Support network (including mobile) operator policy enforcement objectives, such as the need to make policy decisions on traffic that passes through the network.
18. Support access through multiple firewalls and multiple policy enforcement functions placed within the traffic flow between a subscriber's IMS application and their IMS network services.
19. Support access through NAT devices and multiple NAT(s) as may be placed within the traffic flow between a subscriber's IMS application and their IMS network services.
20. Support access through HTTP proxies.
21. Allow a NIMSFW to detect IMS traffic shall not:
    - add considerable overhead:
    - nor compatibility problems:
    - nor deviate from standards:
    - nor require extensions to standard implementations to the entities communicating over a NIMSFW.

Editor's note: Considerable overhead needs to be defined.

The solution(s) **should**:

1. Consider the detectability of traffic through firewalls or other policy enforcement functions and the complexity of such detection.

The solution **may**:

1. Support capability for the UE to selectively route certain IP traffic associated with IMS services over the firewall traversal mechanism.

6.2 Security requirements

The solution **shall:**

1. Comply with Lawful Intercept and other regional regulatory requirements
2. Ensure that mandatory IMS access security for the control plane is preserved
3. Ensure that the optional IMS security for user plane is preserved
4. Ensure that the introduction of FS_FIRE shall not have any negative impacts on the security of the protected security zone(s) behind the NIMSFW and shall not have negative impacts on the security of the terminals.

- Editor's note: The impact on emergency calls is for further study
- The impact on IMS client authentication is for further study
- Additional security features that may be required at the tunnelling level should be further studied.
- Device Impact of iFire should be further studied

6.3 Firewall and policy considerations

Firewalls in this context are a type of policy enforcement function that exist in the traffic path between an IMS subscriber's IMS application and an IMS service provider's IMS core that act upon the IMS application's IP traffic.

The policy enforcement function firewalls provide in this context is whether to allow traffic to pass or to deny traffic, which may or may not correspond to the IMS application's IP traffic. There may be varying desires such as to block or permit all traffic including the IMS application's IP traffic; or to allow traffic for some in the network authorized to use IMS applications while denying for others; or to allow traffic to flow to or from particular IMS service providers while denying to others to enforce particular roaming agreements or business arrangements. There may be other types of policy devices, such as 3GPP TDF or others outside the domain of 3GPP that perform packet inspection, that interact with other policy enforcement functions such as PCRF or AAA servers that then effect policy enforcement on IP traffic or other devices including UE that are not typically thought of as firewalls but have the same policy enforcement function to deny or allow traffic to pass. Firewalls may be integrated into 3GPP equipment such as GGSN or P-GW, or may be placed on the SGi/Gi interface.

In this context, the IMS application is assumed to be an IMS subscriber's application customarily provided by an application conformant to 3GPP specifications that support the Gm reference point (CSCF-UE) that used to provide services to subscribers such as voice, presence, video, etc. and the associated signalling (e.g. SIP) and media (RTP/RTCP) with such IMS applications.

The following three cases are identified with respect to the IP access types available to an IMS application and placement of firewalls in the IMS application's IP traffic path in this context:

Case I: Via Generic IP

The IMS application may reside on an IMS subscriber's TE as an NGN-UE employing the Gm reference point that provides IP access by any means, e.g., PC, tablet, mobile device, or embedded device and may or may not have 3GPP UE capabilities or assume any special relationship with any 3GPP UE capability available, e.g., it may simply access an IP network that may ultimately provide connectivity to an IMS service provider via any generic 802.3, 802.11, 802.16, 3GPP2, CDMA2000®, TISPAN, other non-3GPP specified technology or leverage any 3GPP UE capability other than access to an IP network as a Generic Entity (GE). TE is as defined in Annex L 33.203. IP access would be as provided by one or more Generic Entity (GEs) per Annex L 33.203.

/End Case I

Case II: Via utilizing Gi/SGi

An IMS application may be co-resident with or provided by a 3GPP UE which in turn provides IP access to an IMS service provider's IMS core through access to an IP network via SGi/Gi interfaces.

NOTE: The preceding sentence applies to
WLAN Direct IP access defined in TS 23.234 [11],
WLAN 3GPP IP access defined in TS 23.234,
Generic Access Network (GAN) defined in TS 43.318 [6],
Trusted and Untrusted non-3GPP access defined in TS 23.402 [13], and
3GPP radio access technology that provides PS access (GPRS, EDGE, UMTS, HSPA, LTE, LTE-A).

Access may be a possibility where SGi or Gi are the Internet or some other network where there is no relationship between the IMS service provider and 3GPP mobile operator. The arrangement on trusted non-3GPP access and WLAN Direct IP access between the access network and the 3GPP mobile operator providing SGi and/or Gi is such that SGi and/or Gi are ultimately presented to the network by the 3GPP mobile operator.

/End Case II

Case III: Via utilizing WLAN Direct IP access or trusted non-3GPP access where IP access is provided to the Internet or some other network directly from an WLAN AN or non-3GPP network viewed to be an access network (AN)

Both WLAN Direct IP access and trusted non-3GPP access provide the capability to access an IP network—such as the Internet--other than SGi or Gi as currently defined where traffic directly ingresses or egresses an Access Network (AN) that provide access to an IMS service provider

/End Case III

The following diagram is representative of the above 3 cases.

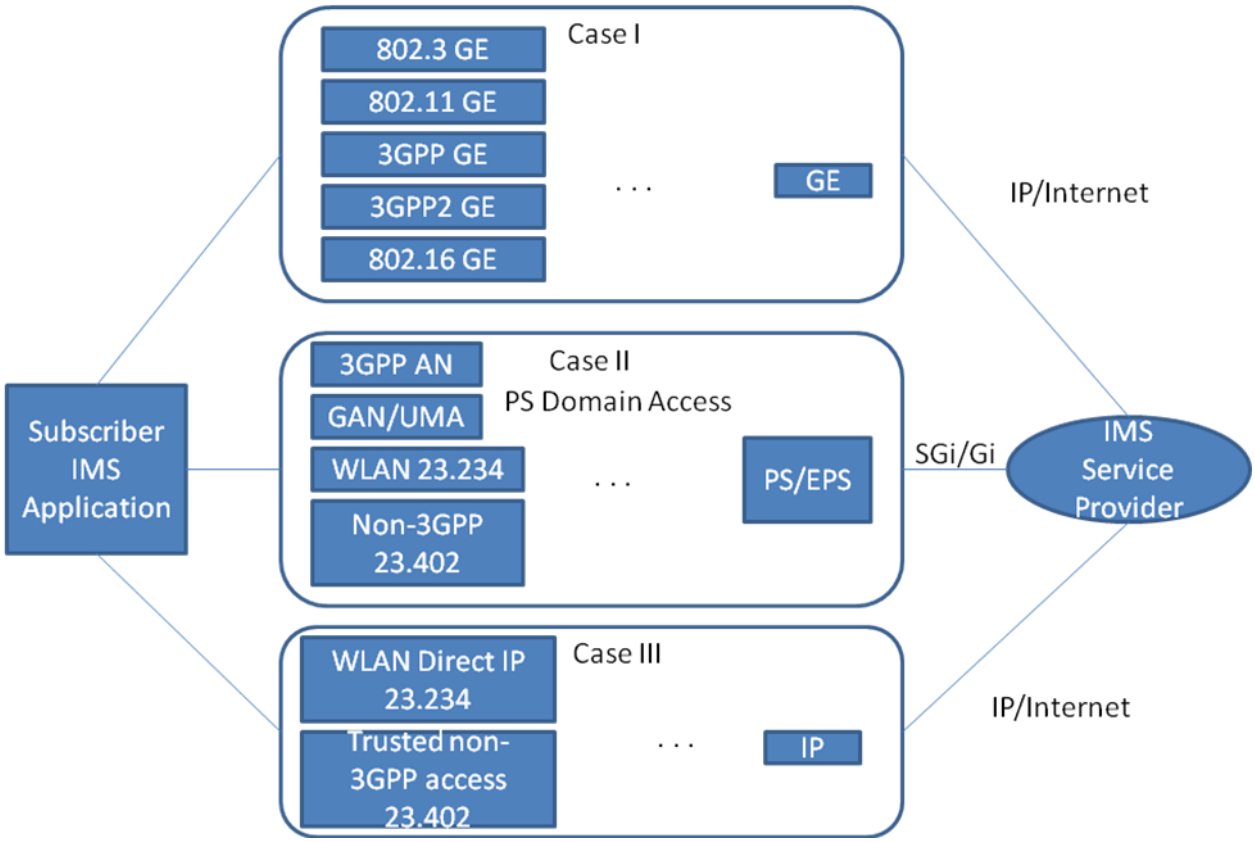


Figure 6.3: Access of subscriber IMS applications

In cases I and II, certainly firewalls and other policy enforcement could exist in a mobile operator's network or anywhere in the network that block a subscriber's IMS application IP traffic whereas the IMS service provider's goal may be the opposite. In case III, firewalls and other policy enforcement could exist within an AN that could block a subscriber's IMS application IP traffic.

It is assumed the IMS application has sufficient privilege to execute on an NGN-UE, 3GPP UE, or TE. It is assumed the IMS application's IP traffic is permitted to egress or ingress the subscriber's UE. There is the possibility that the UE or GE??? could have a firewall or some other policy enforcement function that blocks an IMS application's IP traffic.

An IMS service provider may be a 3GPP mobile operator but is not assumed. IMS service provides could be mobile operators, fixed network operators, Telco's, application service providers, enterprises, and so on. No business or special relationship between the IMS service provider and the rest of the network is assumed other than that which supports IP access. If there is a special relationship and/or additional interfaces, such as policy, charging, security, and so on, then these are presumed to follow 3GPP specifications (az: there are NO 3GPP Recommendations). The IMS service provider is often accessible by the Internet in addition to other IP networks that support a private or other privileged interconnect, such as enterprise networks, WLAN ANs, other mobile networks (3GPP, 3GPP2, 802.16-based, etc.), connection from a broadband fixed network, and so on.

A firewall operator is an entity which operates a firewall for the purposes of effecting policy enforcement of permitting or denying IP traffic within a network as well as traffic which may ingress or egress a given network by the owner of the network. These network owners may be (non-exhaustive):

1. Residential consumers
2. Enterprises
3. 3GPP-based mobile operators
4. non-3GPP mobile operators
5. WiFi access providers that provide roaming or hotspot access
6. ISPs that provide interconnection between a residential consumer or enterprise and another IP network or Internet
7. Transport or transit providers that provide interconnection between ISPs and operators or between operators (e.g., GRX, IPX, transit exchanges, peering exchanges, …)
8. IMS service providers that are 3GPP or non-3GPP mobile operators
9. IMS service providers that are not mobile operators, e.g. fixed network operators

The network operator and firewall operator may be the same entity or not. It is also possible that a firewall may be present on multiple networks, e.g. a residential gateway that exists on both the consumer's network and an ISP network where both the consumer and ISP may singly or jointly administer policies and have control over the respective policies for each network where a firewall is present.

7 Overview of existing 3GPP compliant solutions

Editor's notes: This clause discusses the existing firewalls traversal techniques suggested in the 3GPP specifications and the restrictions imposed by these techniques on IMS traffic.

7.1 STUN, TURN and ICE

7.1.1 Introduction

3GPP TS 23.228 [9], Annex G specifies the use of STUN, TURN and ICE for NAT traversal in IMS networks.
Also, 3GPP TS 24.229 [7] further specifies the use of these mechanisms to provide NAT traversal in the IMS networks.
The following clause briefly explains these mechanisms and explains the limitations these mechanisms have for traversing certain kind of FW/NAT devices in the IMS environment.

7.1.2 Session Traversal Utilities for NAT (STUN)

STUN (RFC 5389) is a standardized set of methods, including a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications.
STUN is a tool to be used by other protocols, such as TURN, and it defines an extensible packet format.

The STUN protocol allows applications operating through a Network Address Translator (NAT) to discover the presence of a network address translator and to obtain the mapped (public) IP address (NAT address) and port number that the NAT has allocated for the application's User Datagram Protocol (UDP) connections to remote hosts.
The protocol requires assistance from a 3rd-party network server (STUN server) located on the opposing (public) side of the NAT, usually the public Internet.

In addition to using protocol encryption via TLS, STUN also has built-in authentication and message-integrity mechanisms via specialized STUN packet types. When a client has discovered its external address, it can use this as a candidate for communicating with peers by sharing the external NAT address rather than the private address (which is, by definition, not reachable from peers on the public network). If both peers are located in different private networks behind a NAT, the peers must coordinate to determine the best communication path between them. Some NAT devices may restrict peer connectivity even when the public binding is known.

7.1.2 Traversal Using Relay NAT (TURN)

TURN (RFC 5766) protocol enables a TURN client located on a private network behind one or more Network Address Translation (NAT) to allocate a transport address from a TURN server which is a designated device on the internet.
This allocated transport address can be used for receiving data from a peer.
The peer itself could be on a private network behind a NAT or it could have a public address.
Refer to RFC 5766 for more information on TURN and its operation.

7.1.3 Interactive Connectivity Establishment (ICE)

ICE (RFC 5245) is a technique for NAT traversal for UDP-based media streams (though ICE can be extended to handle other transport protocols, such as TCP) established by the offer/answer model (RFC 3264).
ICE is an extension to the offer/answer model, and works by including a multiplicity of IP addresses and ports in SDP offers and answers, which are then tested for connectivity by peer-to-peer connectivity checks. The IP addresses and ports are included in the Session Description Protocol (RFC 4566) and the connectivity checks are performed using the revised STUN specification (RFC 5389).

ICE concept can be summarized using the following bullet items:

- Gather all candidates using STUN/TURN mechanism.
- Order them by priority.
- Communicate them to the caller in Session Description Protocol (SDP).
- Do connectivity checks.

- Stop when connectivity is established.

7.1.4 Conclusions on STUN, TURN and ICE

Combination of STUN, TURN, and ICE can solve most of the UDP firewall traversal issues via:

- Obtaining a server reflexive address via STUN
- Obtaining a relayed address via TURN
- Telling the other party about these addresses via ICE
- Making connectivity checks
- Obtaining peer reflexive addresses

Summary:

- STUN, TURN, ICE over the default ports **achieve** firewall traversal of NAT/FW types 1-4, and NIMSFW type 6 (TCP Restricted NAT/FW).
- STUN, TURN, ICE over the allowed TCP ports (e.g. 80 or 443) **achieve** firewall traversal also of NIMSFW types 5 and 7 (Port Restricted NAT/FW and Specific Port TCP Restricted NAT/FW).
- STUN, TURN, ICE **does not achieve** firewall traversal of NIMSFW type 8 (Firewall with HTTP Proxy), unless the TCP connections are set up with HTTP CONNECT.
- STUN, TURN, ICE over TLS on the allowed TCP port (e.g. 443) **achieve** firewall traversal also of NIMSFW type 9 (Firewall with Deep Packet Inspection (DPI) capability and Application Awareness).

7.2 IPsec / IKE v2

Encapsulation of IKE and ESP in UDP port 4500 enables these protocols to pass through a device or firewall performing NAT assuming that the port is open.

3GPP TS 33.203 [8], Annex M, 3GPP TS 43.318 [6] and TS 44.318 [10] specify IPsec in ESP-UDP (RFC 3948) encapsulation mode to support NAT traversal for the IMS control plane. However, IPsec ESP-UDP packets do not traverse strict TCP firewalls since the transport protocol for IPsec ESP-UDP mode is UDP. Also, the default port for IPSEC while running in the ESP-UDP mode is UDP port 4500 and hence "port restricted FW/NAT" could block the IPSEC traffic and "specific port TCP restricted FW/NAT" definitely blocks the IPsec ESP-UDP packets. In addition, many firewalls are configured explicitly block IPsec traffic in turn blocking???? the IMS traffic carried over IPsec.

8 Candidate solutions

Editor's notes: This clause discusses the candidate solutions for traversal of IMS traffic through NIMSFW and also satisfies all the requirements listed in the earlier clause.

Editor's note: It is FFS whether the solution proposals would require IETF standardization or whether 3GPP may choose to define the new protocols themselves.

8.1 Common procedures

This clause focusses on the common procedures which could be followed by all the candidate solutions for solving the NIMSFW traversal issue for IMS services.

The candidate solutions must be invoked only when the existing 3GPP access and FW traversal mechanisms are unable to provide a path for the IMS services through the NIMSFW. The candidate solutions should also include the HTTP CONNECT procedure to allow the IMS applications to traverse NIMSFW with HTTP Proxy. The HTTP CONNECT mechanism must be invoked before sending any IMS traffic to ensure uninterrupted delivery of IMS traffic.

8.2 Tunneling solutions transparent to the existing IMS core

This clause describes a class of solutions rather than one specific, single solution. In this class of solutions traversal of NIMSFWs is achieved by means of tunnels. There is a Tunnel End-Point (TEP) on the IMS core side of the last traversed NIMSFW in the direction from UE to IMS core. (There may also be two different TEPs, one for control traffic, the other for media traffic – this is discussed in NOTE 4 below.).The TEP is a function that does not interact with any existing IMS core function. In this way, requirement 6 from clause 6.1 is fulfilled.

Assuming that firewall traversal for IMS services is not restricted by policies of premises or network firewall operators as mentioned in clauses 4.2 or 4.3, access to the IMS proceeds as follows:

(1) The UE checks whether the NIMSFW traversal procedure needs to be invoked. Which method is used for this does not matter, as long as the method eventually returns the result YES or NO.
If NO, IMS access proceeds as currently specified.
If YES, the traversal proceeds as described in steps (2) – (6).

(2) The UE sets up a tunnel ending at the TEP.

(3) The UE sends IMS control plane traffic (SIP) destined to the P-CSCF through the tunnel. For this, the IP packets transporting the control plane traffic are encapsulated according to the tunnel protocol that is used.
The TEP decapsulates the traffic and forwards the original IP packets towards the P-CSCF, based on IP routing information.

(4) Control traffic from the P-CSCF towards the UE is forwarded by the P-CSCF towards the TEP based on IP routing information.

(5) The UE and the IMS core execute the IMS procedures as defined by current specifications. Note that this may involve a TLS connection between UE and P-CSCF, depending on the policies set by the IMS core and the capabilities offered by the UE. In this case, the TLS connection would pass through the tunnel between UE and TEP, but otherwise the two tunnels would be unrelated.

(6) When a media session is established, media is also forwarded through the tunnel. At the UE side, the IP packets transporting the media are encapsulated according to the tunnel protocol that is used. The TEP decapsulates the traffic and forwards the original IP packets along the media path, based on IP routing information.
As above, media towards the UE also reaches the TEP based on IP routing and forwarding and is forwarded through the tunnel by the TEP.

NOTE 1: The UE needs to know the IP address of the TEP. This address, or a server name from which it may be discovered, may be provisioned at the UE.

NOTE 2: Downlink traffic (traffic to the UE) to reach the TEP may be facilitated as follows: There is a pool of IP addresses from which the TEP allocates one to the UE. This address is used as source IP address for IP packets from the UE that are forwarded by the TEP towards the IMS core. The routing information on the IP layer of the network comprises the information that traffic to these IP addresses from the TEP's pool has to be routed to the TEP. (For example, the TEP may advertise these addresses using an IP routing protocol run in the network.)

NOTE 3: Using a different tunnel at the same TEP for media is possible. To facilitate this, different IP addresses may be assigned to the UE for control and for media traffic. It may also be possible to use the same address, but then forwarding at the UE and the TEP must not be purely based on the destination address but must also take into account an additional criterion like a DiffServ code point, a flow label or the layer 4 port information.

NOTE 4: Using two different TEPs (one for control and one for media) is possible. The UE has to establish a tunnel to the media TEP at the beginning of step (6) in this case. One IP address for control traffic destined to the UE and another IP address for media traffic destined to the UE is used in this case, which facilitates IP forwarding through each of the different tunnels.

Remarks on the efficiency of the proposed solution:

While the existing IMS core functions do not know about the firewall traversal method, the UE does. If the UE uses the firewall traversal, and the applied tunnel already provides the desired protection features, the UE may – within the limits of the security policies enforced by the network – avoid using similar IMS protection mechanisms between UE and core in order to avoid the effort of double protection. Namely, the UE may not request e2ae media plane protection as specified in 3GPP TS 33.328 [14], thus avoiding double protection of the media traffic.

With respect to control traffic, the P-CSCF may enforce the usage of a protection mechanism, like a TLS connection between UE and P-CSCF, leading to double protection between the UE and the TEP if a protected tunnel is used for firewall traversal. This may be considered not an issue at all when the UE is fully capable to perform the required processing. (Note that the processing capacity required in the UE for the protection of control traffic is expected to be small compared to that required for media traffic protection.)

Editor's Note: The statement "(Note … protection.)" is ffs especially when considering Subscribe/Notify messages used with the presence feature in the RCS scenario.

In other cases, it may be desirable to avoid the additional protection inside the protected tunnel. This may be achievable still without the P-CSCF being aware of the traversal mechanism. E.g. if the P-CSCF supports protection policies depending on IP address ranges, the P-CSCF may be configured not to require protection if the UE IP address is in a certain IP range, this IP range being the pool of IP addresses assigned to UEs by the TEP terminating the protected tunnel, as described in NOTE 2 above.

Editor's note: It is ffs which protection features, encryption, integrity, or none, are required for the tunnel between UE and TEP so that the purpose of NIMSFW traversal can be fulfilled. Note that IMS already specifies protection methods for both signalling and media.

Editor's note: It is ffs which of the tunneling methods proposed to SA3 can be used as the generic tunneling method described in our proposal.

8.3 Reuse of existing solutions

Before introducing new nodes or functionality, there is a need to study if the current mechanisms can be extended to support traversal of most or all types of restrictive firewalls. This candidate solution achieves firewall traversal by reusing existing solutions without introducing any new network elements. Existing nodes are required to support TLS on port 443 (the default port of HTTPS). This is already allowed by existing standards.

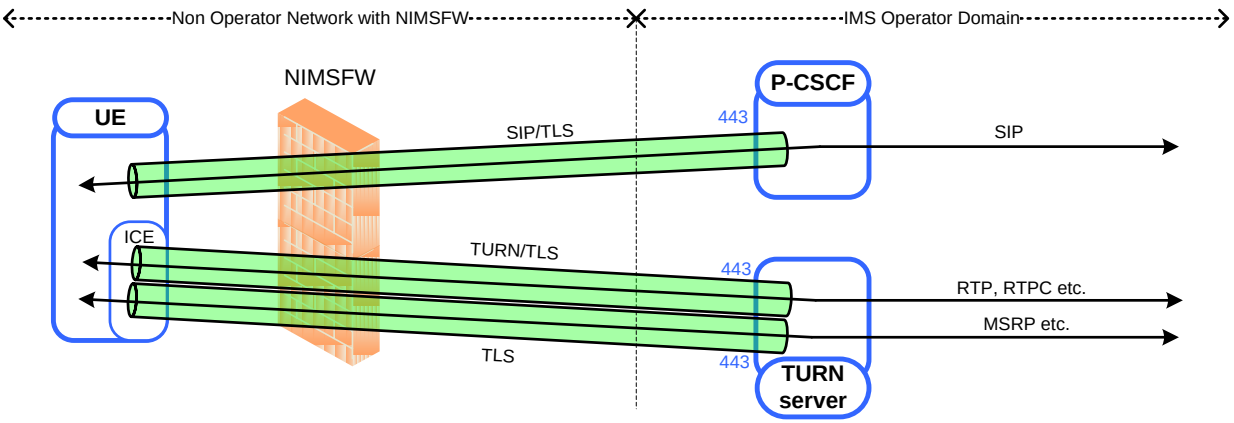


Figure 8.3: Architectural overview

The solution relies on the use of existing TLS connections:

- IMS control plane (SIP): One for the Gm interface.
- IMS media plane (RTP, RTCP, MSRP, etc.): One for the TURN control connection and one for each allocated TURN TCP connection.

The TLS connections are maintained by sending keep-alive messages as described in TS 24.229 [7].

The additional requirements on the UE, P-CSCF and TURN server is as follows.

1) UE to support the option to transport SIP over TLS, and for P-CSCF to support SIP over TLS on port 443 instead of the default SIP TLS port.

   NOTE 1: This is in full accordance with RFC 3261, TS 24.229, and TS 33.203 [8].

   NOTE 2: Before Rel-12, TS 33.203 specifies in its Annex O.2.2 that the TLS session set-up comprises as its first part a REGISTER not yet secured by TLS that includes a sip-sec-agree negotiation resulting in TLS to be used subsequently. In the solution proposed here it is however required that a TLS tunnel is established before any SIP traffic is exchanged. In this respect, the proposed solution is not covered by TS 33.203 before Rel-12.

2) UE to support ICE with TURN over TLS, and for TURN server to support TURN over TLS on port 443 instead of the default TURN TLS port.

   NOTE 3: This is in full accordance with RFC 5245 and RFC 5766.

3) UE to support normal web proxy procedures (HTTP CONNECT) to set up TLS connections on port 443 to the P-CSCF and TURN servers.

   NOTE 4: One HTTP CONNECT request is needed for each TCP connection. Where HTTP_CONNECT is implemented in the UE is implementation specific.

While RFC 5766 only allows UDP allocations, RFC 6062 defines TCP allocations for TURN. The solution can therefore be used for both UDP and TCP based IMS media plane protocols.

The number of TLS connections to the TURN server (and therefore the number of HTTP_CONNECT) depends on the IMS service and the protocols used. For immediate messaging, a single TLS connection is needed, whereas for MSRP three TLS connections are needed.

The UE proceeds as follows:

1) The UE tries to register according to normal procedures, if this fails the UE continues according to 2).

2) The UE tries to register using alternative procedure for NAT traversal UE, if this fails the UE continues according to 3).

3) The UE tries to register using alternative procedure for NAT traversal UE, but sets up TCP connections on port 443 using HTTP_CONNECT as described above.

NOTE 5: This requires the P-CSCF to accept TLS connections without preceding negotiation, which is not covered by existing 3GPP specifications before Rel-12.

When changing access, the existing procedures for session continuity as described in TS 24.237 [12] still apply.

The solution supports both encrypted and unencrypted connections.

- If confidentiality is desired, a cipher suite with encryption (e.g. TLS_RSA_WITH_AES_128_CBC_SHA) is negotiated. This achieves traversal for all NIMSFW types (1-9).

- If confidentiality is not needed, a cipher suite with NULL encryption (e.g. TLS_RSA_WITH_NULL_SHA) is negotiated.). This achieves traversal of NIMSFW types 1-8.

As the solution just requires the P-CSCF and TURN server to support TLS on port 443, and the P_CSCF to accept TLS connections without a respective preceding negotiation, he solution has little impact. Existing IMS authentication mechanisms can be reused.

8.4 Tunnelled Services Control Function (TSCF)

This candidate solution introduces a new network element called a Tunneled Services Control Function (TSCF). TSCF relays IMS messages to UE using managed TLS tunnels to communicate to UE via embedded Tunneled Service Element (TSE). TSCF relays P-CSCF messages and IMS application on the UE points at a standard TLS tunnel on the TSCF. The Tunnel could be shared between multiple applications (SIP, RTP, MSRP etc.).

NOTE: TLS refers to the connection created using the protocol specified in RFC 2246, RFC 4346 or RFC 5246.

Figure 8.4-1 below describes a possible deployment model in which all application traffic (including media) is tunneled using TLS Tunnel.

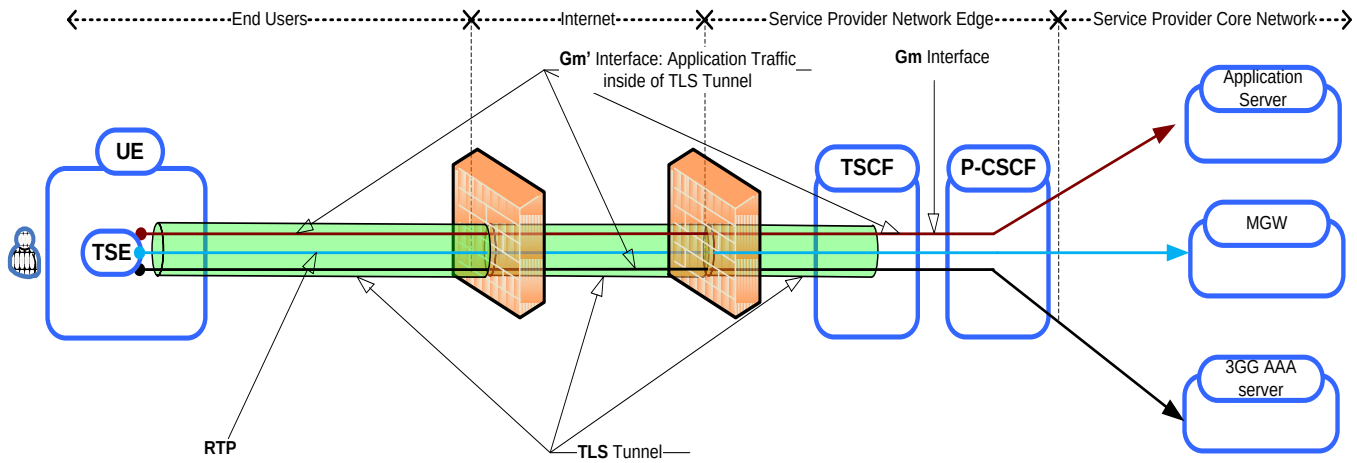


Figure 8.4-1: Deployment model: P-CSCF with TSCF. Gm' Interface, TLS tunnel model

Figure 8.4-2 below describes changes to IMS Application. During the tunnel negotiation phase, the TSCF assigns a remote IP (inner) to the UE and all the protocols on the IMS application on the UE use the remote IP address to correspond with the core network element. The remote IP address can be locally configured on the TSCF or TSCF could obtain the remote IP address through a 3GPP AAA server in the IMS network. TSCF tunnels/de-tunnels the IMS packet and forwards the inner packet from the tunnel to the core network. Once the TSCF forwards the IMS messages to the P-CSCF, P-CSCF, it handles the IMS messages as specified in 3GPP TS 24.229 [7].

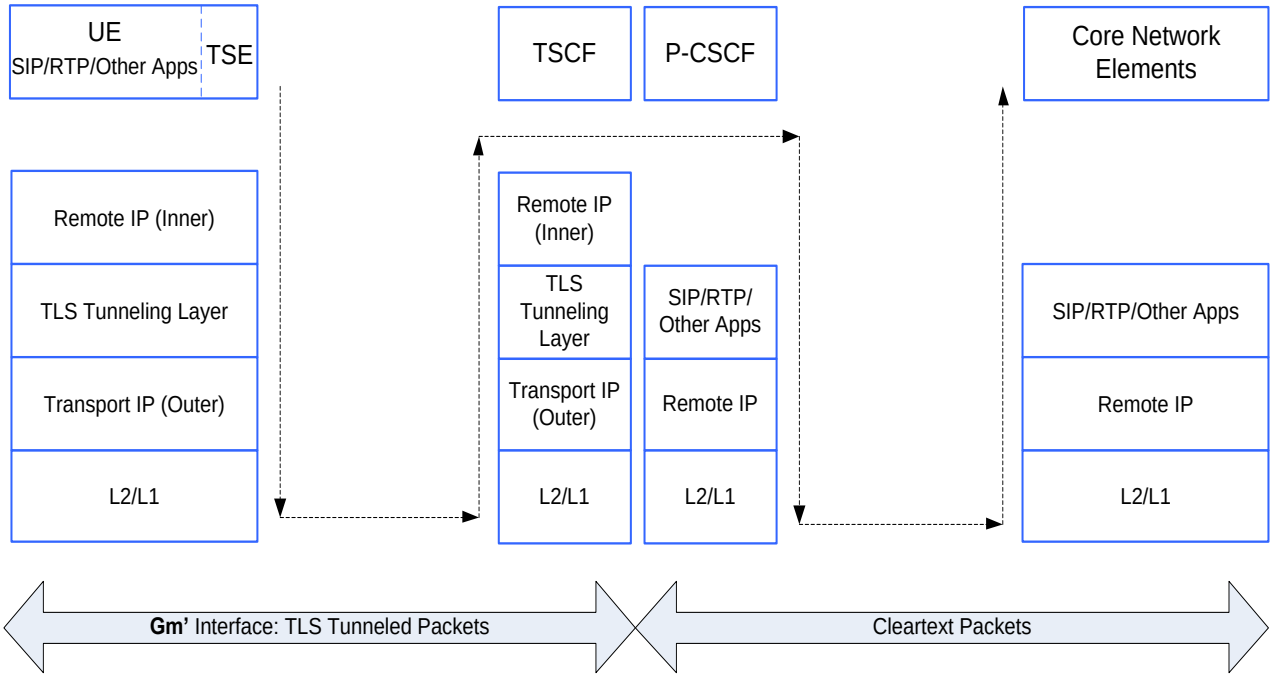


Figure 8.4-2: Protocol stack for TSCF function

8.4.1 Packet format

All packets from the UE will be comprised of "inner" and "outer" parts separated by TLS Tunnel header. See Figure 8.4.1-1 below for the packet format.

The "outer" headers will contain TSE and TSCF L3/4 information.

The "inner" headers will contain IMS application/P-CSCF headers.

The existence of the tunnel will be transparent / orthogonal from the Application/P-CSCF layer. In other words, "inner" IP address will be unmodified to accommodate TLS tunnel (as if tunnel does not exist).

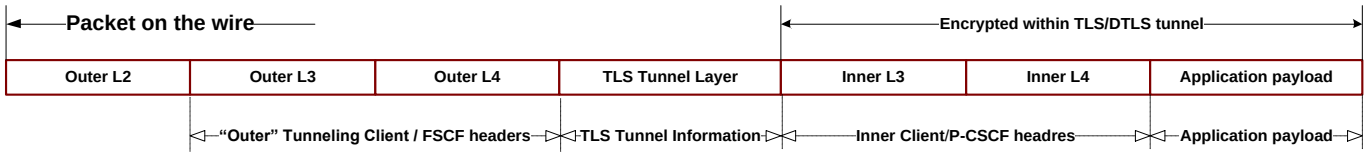


Figure 8.4.1-1: Simplified Payload Packet structure

In addition to a Payload Packet (PP), an optional Control Message (CM) packet is available.

The CM is used to negotiate keep alive mechanism, protocol version, UE Inner IP assignment, negotiate header compression and Authentication mechanisms. Figure 8.4.1-2 below describes the overall CM packet structure.

TSCF keep-alive mechanism is very similar to the double CRLF mechanism as specified in RFC 5626 and is less expensive than the STUN based mechanism as specified in RFC 3489.

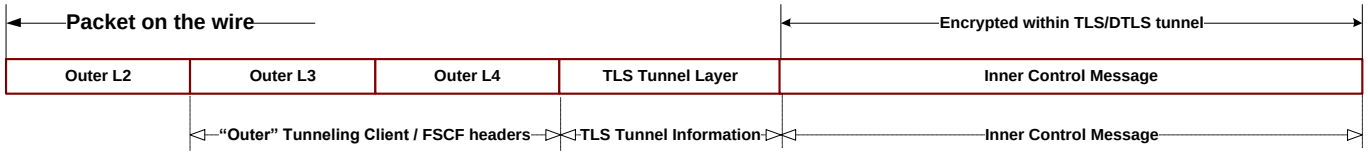


Figure 8.4.1-2: Control Packet structure

8.4.2 Detection and traversal of NIMSFW

The proposal suggests the following mechanism to detect the presence of a NIMSFW and traverse it.

1. The IMS application will first try to register according to normal procedures specified in the 3GPP spec TS 24.229. If this fails, then it may try using alternative procedure specified in 3GPP for NAT traversal. If this also fails, then continue to step 2.

2. If a non-transparent HTTP proxy is configured, The TSE should send a HTTP CONNECT method (RFC 2616) to the HTTP proxy in the network, to port 80/443. Once the TSE gets a successful response to the HTTP CONNECT, TSE should move to step 3. If the TSE does not get a successful response to HTTP_CONNECT, this indicates misconfiguration in the network and it is not possible to run the IMS services through this network.

   If there is no non-transparent HTTP proxy configured in the terminal, TSE should go directly to step 3.

3. TSE should try to establish a TLS tunnel to destination port 80/443 on the TSCF. If the establishment of the TLS tunnel is successful, TSE should indicate to the IMS control plane and user plane protocols the presence of the NIMSFW. At this point, all the IMS protocols must send all their traffic over the established TLS tunnel. Optionally, if the end to end security is not enabled, IMS protocols could disable security at the protocol level since the TLS tunnelling mechanism will provide packet level encryption and authentication mechanism.

   If the establishment of TLS tunnel is not possible, this indicates misconfiguration in the network and it is not possible to run the IMS services through this network.

The following flowchart describes TSE connection state machine:

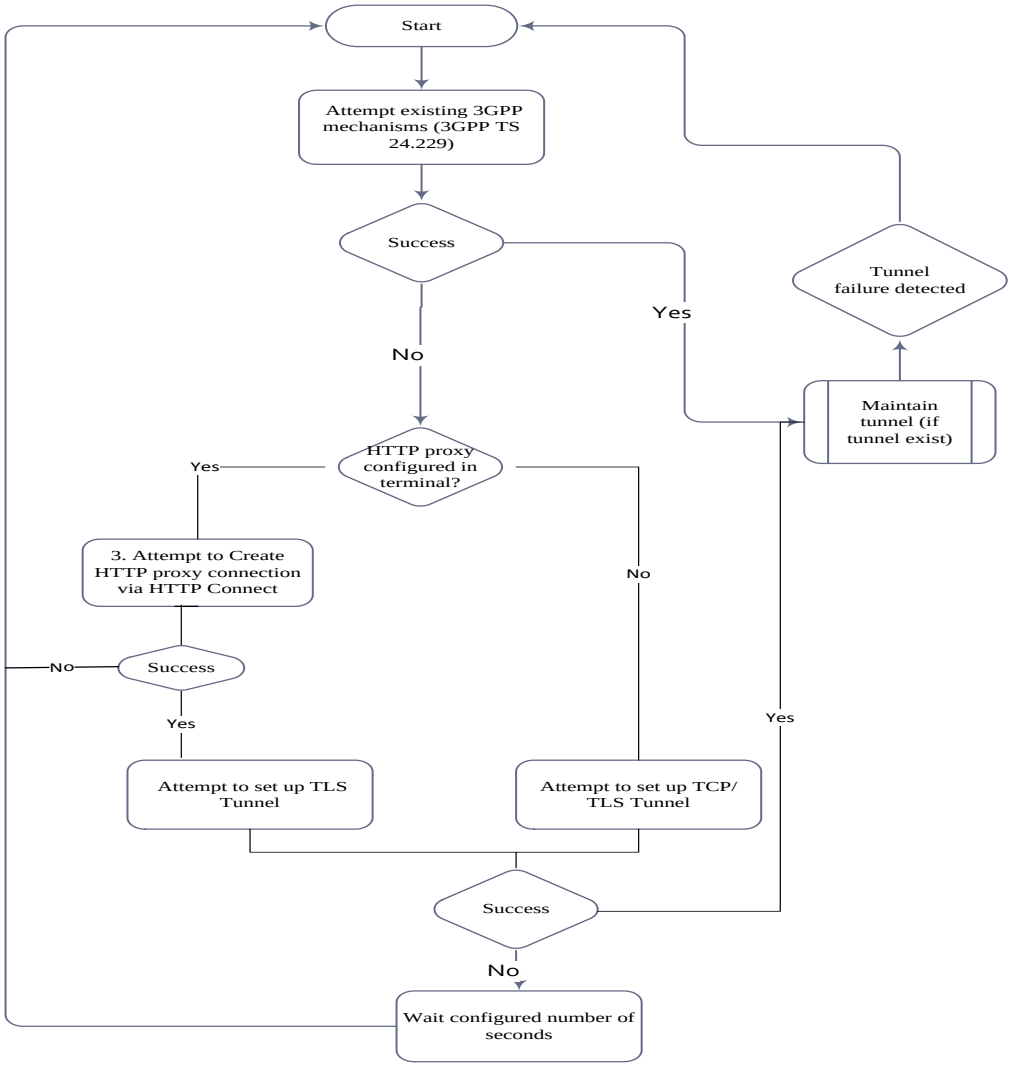


Figure 8.4.1-2: TSE connection state machine

8.4.3 Overhead and performance impact with this solution

This clause compares the overhead and performance of running TLS tunnel with IPSEC mechanism which is recommended in the 3GPP specs for FW/NAT traversal.

The proposed tunnelling mechanism uses TLS to carry the data. The data is carried in TLS records over the wire and the TLS record is of length 5 bytes. Since the data is encrypted and integrity protected, there is an additional overhead that is incurred. Let's assume that the cipher suite negotiated between the client and the server is TLS_RSA_WITH_AES_128_CBC_SHA, which is mandatory for TLS1.2 and hopefully will be commonly negotiated going forward. Since AES is a block cipher, it requires the data to be sized in multiple of the block size.
TLS 1.0 (RFC 2246) defines the encrypted data with block cipher as:

```
block-ciphered struct {
    opaque content[TLSCompressed.length];
    opaque MAC[CipherSpec.hash_size];
    uint8 padding[GenericBlockCipher.padding_length];
    uint8 padding_length;
} GenericBlockCipher;
```

Since most implementations don't use compression, it is assumed that the data is the same size. The MAC in this case is computed using SHA1, so the size is 20 bytes. AES128 has a block size of 16 bytes, so the maximum padding that can be added to the data is 15 bytes. The total overhead of the TLS encrypted data is about 40 bytes (20 + 15 + 5). The total overhead of adding an additional IP header and the TCP header is additional 40 bytes. So, for every packet, this TLS tunnelling mechanism on an average adds 80 bytes per packet.

The average overhead of running IPSEC ESP UDP mode will be 73 bytes(20 byte new ip header by ESP in tunnel mode + 8 byte UDP header + 16 Byte ESP Header + 2Byte ESP Trailer + 12 byte ESP Authentication data + 15 bytes for maximum padding for AES).

It is clear from the above calculation that per packet overhead for TLS tunnel is very similar to that of IPSEC in ESP - UDP mode.

Given the fact that all the mechanisms (TLS and IPSEC) use AES (128/256) for encryption and SHA1 for authentication, the performance impact of running TLS tunnel should be very similar to that of running IPSEC tunnels.

The following table gives a summary of comparison between IPSEC, SIP/TLS and SRTP with TLS.

Table 8.4.3: Comparison between IPSEC, SIP/TLS and SRTP with TLS

Metric / Solution	Packet Size		Computational needs		Network Design Complexity		NIMS FW Traversal	Security	Application Neutrality
	Overhead	Mitigation	Overhead	Mitigation	Overhead	Mitigation			
IPsec	73 bytes	None	AES and HMAC-SHA1 calculation	SIP/TLS and SRTP	MTU should be tuned	None	Not always	Yes	Yes
SIP/TLS/SRTP	40 bytes	None	AES and HMAC-SHA1 Every call requires 2 different negotiations. Maintains 2 different sessions.	None	Multiple secure interfaces	None	Not always	Yes	Media only
TLS tunnel	80 bytes	MTU could be negotiated through the TSCF control packets	AES and HMAC-SHA1	Protocol level encryption could be disabled when TSCF tunnelling mechanism is enabled.	Additional Function: TSCF	TSCF could be integrated into P-CSCF or any other server on the network. TSCF tunnel establishment requires only one session and maintaining one set of encryption and authentication keys. TSCF tunnels could be application aware and provide additional call flow simplification services.	Always	Yes. Always "on" security model minimizes security footprint	Yes

8.4.4 Impact on media release

In the IMS networks, once the P-CSCF negotiates the signalling path through SIP, the P-CSCF could release the media packets (for example, RTP) and allow the media packets to go directly between the UE's. Media release typically happens in the smaller enterprise setup where there are bandwidth limitations with the packets traversing outside the enterprise.

Given that the proposed tunnelling mechanism assigns inner IP address to the UE which is reachable only through the tunnel, media release is not possible with this solution. However, even in the absence of the tunnel, media release may not be possible in the presence of restrictive FW/NAT servers. In addition to the above point, media release may not be compatible with IMS network Lawful Intercept requirements. It shall be noted that for the Lawful Intercept enabled P-CSCF to perform Interception Action; it must have an access to the complete media stream.

8.4.5 Method for IMS FW/NAT servers to block the TLS tunnelling mechanism

In some deployment scenarios, the IMS FW/NAT servers might want to explicitly disable the IMS traffic and the proposed tunnelling mechanism from traversing the FW/NAT server.

8.4.6 TSCF and reachability over restrictive networks for non-IMS services

As mentioned in clause 4.2, the focus of SA1's Stage 1 work on Media Reachability for Users over Restrictive Firewalls (SMURFs) is to find different means to achieve UE access to PLMN IP-based services over restrictive firewalls in non-3GPP accesses. Also, as mentioned in clause 4.2, to achieve traversal through most restrictive firewalls, the solution need to use TCP (set up with HTTP CONNECT), use port 80 or 443, and look like HTTP/HTTPS. In conclusion FS_FIRE is a subset of SMURFs.

TSCF solution makes use of TLS tunnel terminating on TCP port 80 or 443 and also has support for HTTP CONNECT mechanism. For the NIMSFW and for the most restrictive firewalls in scope, the TLS tunnel terminating on port 443 looks exactly like a HTTPS packet thus allowing traversal for all IP based services (both IMS and SMURF) through NIMSFW and the most restrictive firewalls. In the SMURF case, the TSCF function could reside on the ePDG as an alternate tunnelling mechanism to IPSec. To reside on the ePDG, the TSCF function will have to support additional authentication control messages to perform tunnel level authentication on the ePDG.

8.4.7 Impact on changes in network availability

Since TSCF mechanism makes use of TCP/TLS connection, the behaviour of the TSCF for the network changes is very similar to the behavior of running SIP over TCP/TLS in the case iFire (while TSCF is a part of P-CSCF).
When the network changes happen, in the case of running SIP over TCP/TLS and with TSCF, the TCP connection can/will be lost and once there is network connectivity, the TCP connection will be recreated and the operation will continue as specified in the IMS specification TS 24.229 [7] and RFC 3261.

For the SMURFs case, when the TSCF runs as a part of ePDG (for the case of untrustred non-3GPP access), the behaviour of TSCF tunnel is similar to the behavior with IPSEC tunnel as specified in 3GPP TS 23.402 [13].

8.5 Candidate solution — Reuse of IKE/IPsec

8.5.1 Background

Re-use of IKE/IPsec is given consideration due to IKE/IPsec having enjoyed more than a decade of operation to support client-based corporate VPN access. Within 3GPP, IKE/IPsec have enjoyed support across GAN/UMA (TS 43.318), 3GPP system to Wireless Local Area Network (WLAN) interworking (TS 23.234), NDS (TS 33.210), and as well non-3GPP IP access (as in untrusted non-3GPP access in TS 23.402). Many firewalls handle IKE/IPsec without difficulty; however, it is recognized that very restrictive firewalls (such as those that permit TCP traffic only) may block IKE/IPsec. The reuse of IKE/IPsec procedures as well as proposals which address IKE/IPsec's inability to traverse firewalls that permit TCP traffic only merit consideration.

8.5.2 enhanced Security Gateway (eSEG) - Candidate solution

This candidate solution is based upon enhancing Security Gateway (SEG) operations which are modified to address IKE/IPsec deficiencies with respect to UDP transport and as well permit reuse of IKE/IPsec where the firewall allows such to operate. This enhancement of existing SEG functions is termed eSEG. There are other similar enhancements that could be attempted for ePDG, such certainly may be considered under other work, such as SMURFs in Rel-12 to address cases not under consideration for the present document, or as additional candidate solution approaches.

8.5.2.1 eSEG architecture

A function termed an "enhanced SEG" (eSEG) is introduced to support IP tunnelling of existing IMS services within a TCP encapsulation designed to carry IKE and IPsec through restrictive firewalls.

Figure 8.5.2.1-1 illustrates the eSEG in relation to UE, access, and IMS core. A Tunnelling Client (TC) handles the establishment of IKE/IPsec over TCP using a TPKT-like (TPKT') framing.
IKE/IPsec ESP tunnel mode packets that would have been framed over UDP per RFC3948 are now framed over TPKT' over TCP.
This framing of IKE/IPsec packets using TPKT' over TCP is termed TrIKESec (TCP transport for IKE & IPsec). TPKT is defined in RFC968.

Editor's Note: The term TrIKESec is chosen to facilitate discussion of this proposal; TrIKESec is not an industry standardized term.

Editor's Note: It is for further study whether tunnel establishment between the TC and the eSEG need to be authenticated and if authentication is required, what credentials and methods are used.

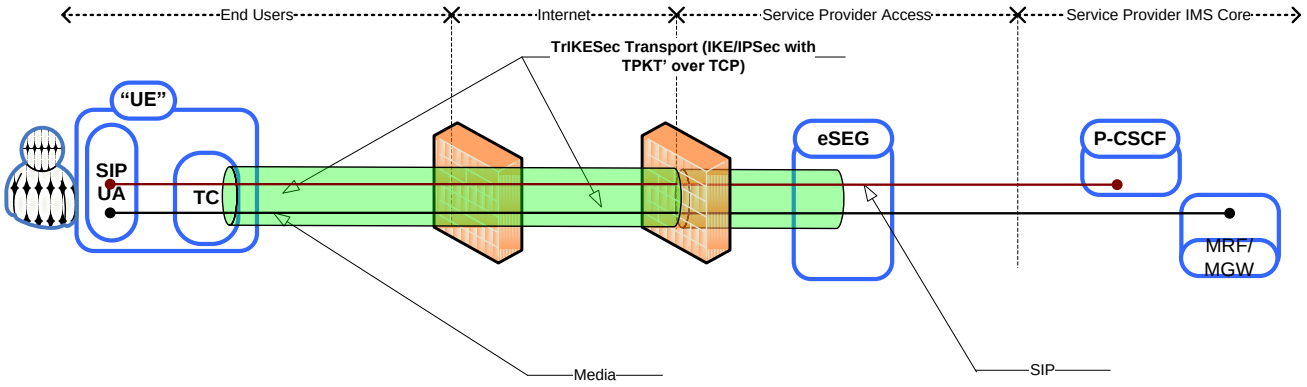


Figure 8.5.2.1-1: Deployment model for eSEG

Figure 8.5.2.1-2 below illustrates transport for SIP, RTP, and other applications following the above method.

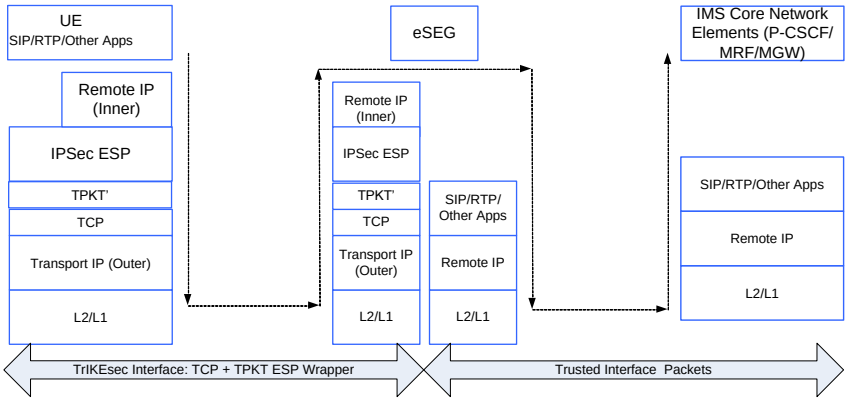


Figure 8.5.2.1-2: SIP, RTP, & other applications transport

Should it not be desirable for SIP (control plane) and bearer (e.g. RTP) to share the same authentication, integrity, and/or confidentiality measures, multiple IPsec SA may be negotiated.

For completeness, IKE carriage follows in Figure 8.5.2.1-3:.

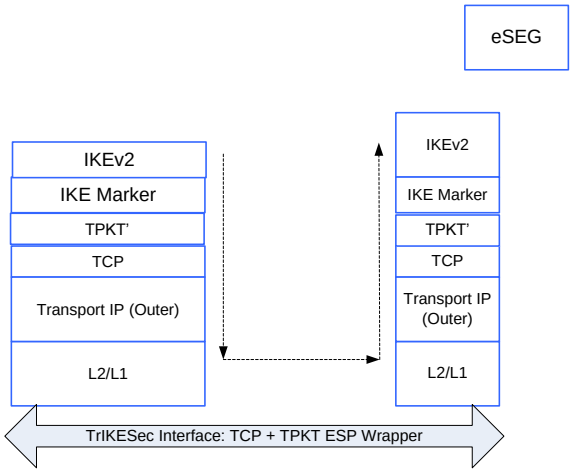


Figure 8.5.2.1-3: IKE carriage

8.5.2.2 eSEG packet format

The following packet formats are used and illustrate the framing for IPsec and IKE packets.

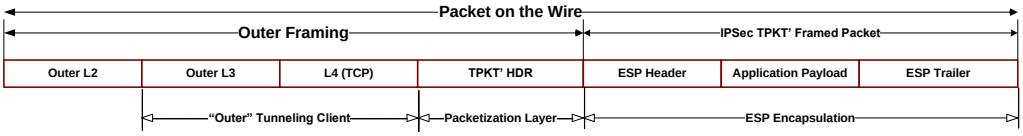


Figure 8.5.2.2-1: IPsec ESP format in TPKT' encapsulation

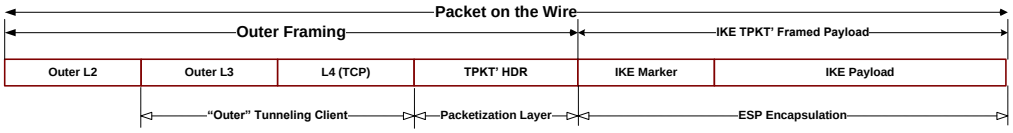


Figure 8.5.2.2-2: IKE packet format in TPKT' encapsulation

IKEv2 features such as key exchange and configuration are preserved.

The TPKT' header is as a TPKT header per RFC983 with version set to 1. The TPKT' header is 4 bytes.

8.5.2.3 eSEG firewall traversal procedures

The following procedures are used to support firewall traversal, both for permissive (firewalls that allow for the passage of IKE/IPsec) and restrictive firewalls (firewalls that do not allow for unmodified passage of IKE/IPsec).
If the UE elects to use this method, perhaps after considering whether other methods of IP access may have already provided access to IMS, the following procedure is proposed for use by the Tunnelling Client (TC).

Step 1. A RFC 5996 IKE negotiation assuming UDP encapsulation of ESP is attempted.
If the IKE negotiation indicates NAT and firewall traversal is successful, IPsec SA are also established.

If step 1 fails, the next step is invoked:

Step 2. A TCP session towards port 80 on an eSEG is attempted. IKE negotiation proceeds with IKE messages encapsulated by TPKT' over TCP illustrated in clause 8.3.2.2. Assuming a successful IKE negotiation, IPsec SA would be created and IPsec ESP tunnel mode packets are framed over TPKT' over TCP.

If step 2 fails due to TCP failing to establish or should IKE or IPsec traffic not be observed, the TC may attempt other methods. The failure of step 2 may indicate the use of HTTP proxies or other policy enforcement which may be interfering with session establishment.

Editor's Note: It is for further study how TrIKESec traverses HTTP proxies; however, it would follow from other solutions that leave the TCP socket open after proxy negotiation may be supported. This may require an initial HTTP connection negotiation to the point where the proxy leaves the socket open.

8.5.2.4 Packet overheads and impact

Assuming the use of IPv4, the average overhead of running IPsec with TPKT' over TCP per packet will be 89 bytes (20 byte IP header + 20 byte TCP header +4 byte TPKT' Header + 16 Byte ESP Header + 2Byte ESP Trailer + 12 byte ESP Authentication data + 15 bytes for maximum padding for AES_128). The TCP and TPKT' framing adds 16 bytes to UDP encapsulation of ESP.

8.5.2.5 Detection of IKE/IPsec with TPKT' over TCP

TPKT' framing is readily detectable and contains a 2 byte header followed by a 2 byte packet length header.
A fixed header has the advantage of not requiring state or network data (such as IP addresses of eSEG) to make local policy decisions regarding these packets.

8.5.2.6 Summary of key properties

IKE/IPsec with TPKT' over TCP has several key properties:

- Application neutrality. It tunnels any IP based protocol.
- Firewall traversal. It traverses firewalls as framed by appearing as TCP port 80 traffic. Many firewalls permit traffic over port 80 given port 80 is used for HTTP.

  Editor's Note: It is FFS as indicated in 8.2.2.3 how traversal is supported where HTTP proxies exist.
- Reuse of IKE/IPsec procedures. IKE/IPsec procedures are reused, there is no need for a new protocol for IP address configuration, dead peer detection, keep alives, address re-keying of long duration sessions, mobility considerations as a result of 802.11 access, and so on.
- Allowance for separate security measures to be applied to SIP signalling and RTP via use of multiple IPsec SA, tunnelled traffic need not share a single authentication, integrity, or confidentiality measure.
- Statically detectable framing format that allow for local policy based decisions and low-complexity packet inspection. The choice of static framing such as implied by TPKT' allows for static and stateless low-complexity decisions.
- TPKT' packet length indication provides a simple UDP packetization emulation that facilitates reuse of IPSec/IKE

  Editor's Note: Details on how this solution handles IP-CAN or other access network availability changes at the UE need to be added.

  Editor's Note: Details on how this solution handles the IMS session is maintenance during IP-CAN or other access network availability changes at the UE need to be added

  Editor's Note: It is FFS as to the keep alive method impact on the UE.

8.6 Media tunneling solutions

Editor's note: It is FFS how and when this solution is invoked and how this solution co-exists with the other IMS firewall traversal solutions.

3GPP specifications allow UE to send signaling and media through different paths, e.g., P-CSCF and IMS-AGW in different locations or using multiple IMS-AGWS. In such cases, it is desired for the firewall traversal function to preserve the control path and data path to avoid unwanted impacts on service and manageability. This candidate solution solves the firewall traversal problem for control plane and data plane independently. It preserves the control path and data path and solves the firewall traversal problem with minimum impact on the IMS architecture.

Since restricted firewall traversal for control using TCP port 80 can solve plane or TLS port 443 for signaling, as explained in clause 8.3 (after adding support for HTTP_CONNECT and detection mechanism for the existence of the NIMSFW), this candidate solution focuses on user plane restricted firewall traversal issue. It introduces a tunnel endpoint called TEP-C for UE and a tunnel endpoint called TEP-S at the Core site. TEP-S and TEP-C are based on ICE/STUN with enhancement explained below. In particular, TEP-S can be integrated with IMS-AGW or the media processing device at core side (such implementation is not uncommon, e.g., STUN can be integrated with media gateway and existing standards define techniques to de-multiplex STUN and other protocols on same port).

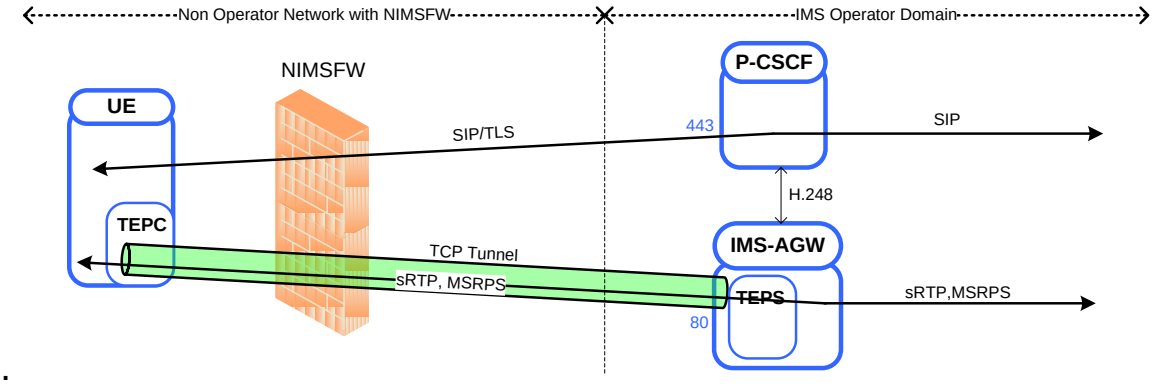


Figure 8.6-1: Architectural overview

This solution assumes that UE knows on which media path TEP-S should be used. One way to do so is for P-CSCF to inform UE whether IMS-AGW (or the media endpoint at core side) supports TEP-S with an ICE attribute extension in SDP. This allows UE to find whether TEP-S can be used dynamically, on a per session basis. It is also possible to configure the UE on which media path to use TEP-S.
If UE finds that the media endpoint at core side does not support TEP-S, it uses TEP-C as ICE agent and use the standard ICE/STUN procedure to solve the traversal issue.
If UE finds that IMS-AGW (or the media endpoint at core side) supports TEP-S, it uses the following procedures:

Editor's note: It is for FFS on whether IETF or 3GPP modifies the ICE protocol for adding the new attribute suggested in this solution

Editor's note: Given that this solution uses TCP based tunnels, it is for FFS that how this solution solves traversal for most restrictive firewalls (like the firewalls with web proxy).

Before making a call, UE find its public address through a STUN request to TEP-S. In this step, TEP-C and TSP-S act as ICE agent at UE and the core side.

When UE makes a call, it uses the public address discovered in step (1) as the media address in SDP (m/c lines or server reflective candidate). This is also the tunnel address at the UE side. TEP-C establishes a TCP tunnel to the TEP-S at core side on TCP port 80. TEP-C can optionally sends a STUN request through the tunnel for tunnel authentication using the short-term credential or long-term credential mechanism defined in RFC5389.

NOTE 1: TLS tunnel can also be used but it increases significant overhead. In addition, it is assumed the media is protected by 3GPP e2ae security mechanisms, so another layer of security is unnecessary.

NOTE 2: Running TLS with null ciphers can minimize the impact of encryption with TLS.

Editor's note: It is FFS how this solution solves SMURF traversal issue.

Editor's note: It is FFS how this solution detects the presence of NIMSFW.

NOTE 3: TCP security can be achieved through STUN authentication or media session identification (media pinhole).

UE and IMS-AGW send / receive media through the TCP tunnel using TCP encapsulation, as shown below:

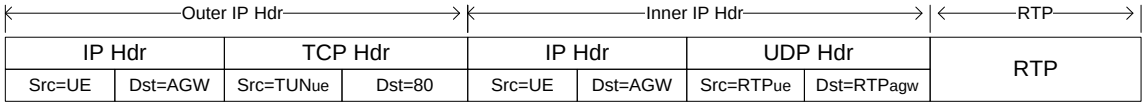


Figure 8.6-2: TCP tunnel encapsulation packet format

In the direction from UE to core, TEP-C on UE captures the outbound media packets, changes the source address to UE's public address, and encapsulates the NATTed packet into TCP tunnel packets. On the core side, TEP-S receives the tunnel packets, removes the tunnel header and sends the inner IP header to the media function at core side. Since the inner packet's source address are NATTed by TEP-C and are identical to the media addresses in UE's SDP, and the destination IP and port are the same as the media address in P-CSCF's SDP, the (src-ip, src-port, dst-ip, dst-port, proto) 5-tuple from the inner packet can uniquely identify the media stream for a call. This is like a normal media processing and the traversal function is transparent to the IMS functions.

Editor's note: It is FFS the impact on the UE with this solution.

In the direction from core to UE, TEP-S captures media packets from core to UE, changes the destination of the packets to the public address found in step (2), and encapsulates the packet in TCP tunnel packets. On the UE side, TEP-C receives the tunnel packets, removes the tunnel header, and changes the destination address to the UE's address, sends the packet to UE. The UE uses the (src-ip, src-port, dst-ip, dst-port, protocol) 5-tuplet to identify media session. The traversal process is transparent to the UE IMS function.

NOTE 4: since TEP-S and the core media function are co-located on the same device and listen on the same interface, it can capture all outbound media packets from core to UE.

NOTE 5: since the inner packets source and destination addresses are also NATTed, topology hiding is achieved in both outer and inner packets.

When a call is terminated, the TCP tunnel is also closed, like the normal ICE/STUN process. In addition, ICE/STUN keepalive mechanism can also be used to check whether a tunnel is still active or need to be closed.

This candidate solution can be viewed as the extension for ICE/STUN based solution. It works when control and user data traverse through different paths, and even when control and user data traverse through the same path, it can be used to optimize the traversal process by using a single TCP tunnel instead of multiple TLS tunnels. By preserving the control and user data paths, this candidate solution minimizes its impact on the IMS architecture that uses this traversal service. If an owner of an NIMSFW wants to explicitly block IMS Services, this can be achieved by blocking the IP address (or range of IP addresses) of the P-CSCF.

9 Co-existence of existing and candidate solutions

The candidate solution must co-exist with the existing 3GPP access and FW traversal mechanisms. Also, the candidate solutions must be invoked only when the existing 3GPP access and FW traversal mechanisms are unable to provide a path for the IMS services through the NIMSFW.

10 Assessment of candidate solutions

Editor's notes: Here we request that the proposed solutions should be evaluated in the SA3 meetings and analysed to see whether it meets the requirements listed in clause 6.

Editor's note: The solution should be studied to understand whether the solution introduces unacceptable delay and jitter.

10.1 Impact on the UE, IMS core and packet core

10.1.1 Impact on UE

Editor's notes: This clause outlines for each solution approach the potential impacts to the terminal, the IMS and HTTP stack.

.

Table 10.1.1: Evaluation with respect to device impact of Solutions for traversal of IMS traffic through NIMSFW

Solutions	characteristic	Device impact			Emphasized satisfaction of requirements	Performance evaluation (eg. Delay, jitter.)
		Changes in UE	pros	cons		
8.2 Tunnelling solutions transparent to the existing IMS core	Tunnel endpoint(TEP) on the IMS core side and UE	UE checks whether the NIMSFW traversal procedure needs to be invoked	Different tunnel at the same TEP for media is possible.	UE has to know the IP address for the TEP	Especially support detection of IMS restrictive firewalls It can separates user and control plane.	Performance depends on tunnelling mechanism (eg. TLS connection)
8.3 Reuse of Existing TLS solutions	Additional requirements on the UE, P-CSCF, and TURN server	UE has to support the option to transport SIP over TLS, TURN over TLS, or TLS connection	Reuse the existing TLS mechanism	UE has to distinguish which procedure it has to follow. It is also possible frequent keep alives.	No changes to the firewall	UE has to try normal procedure, if fail follow the NAT traversal UE procedure
8.4 Tunnelled services control function (TSCF)	New network element TSCF is introduced	During the tunnel negotiation phase, TSCF assign the remote IP(inner) to the UE	Reuse the existing TLS mechanism	UE has to distinguish which procedure it has to follow : normal procedure or NAT traversal UE procedure	Support detection of IMS restrictive firewalls	Additional overhead of TLS encyprted data: header, padding eg. 80 bytes)
8.5 Reuse of IKE/IPSEC	Enhance the security gateway (SEG) operations and similar enhancements for ePDG	For IKE/IPsec implementation , tunnelling client (TC) is in UE	Reuse the existing IKE/IPsec procedures. Tunnelled traffic needs not share a signle authentication or encription mechanism.	UE has to handle frequent keep alives.	Ifire shall not preclude the operation of non-3GPP access methods	Additional overhead due to running IPsec (header, tailer, eg. 89 bytes)
8.6 Media Tunneling Solution	Same as 8.3, plus media tunnelling end point TEP-C and TEP-S at UE and core side	UE checks whether to use existing solutions (8.3) or TEP-S	Support all IMS architectures, no double encryption for media	Tunnel end point needs to intercept packets at network (IP) level	Support user and control planes separation with minimum impact on IMS architecture.	Additional overhead due to TCP tunnelling (IP, TCP header)

Editor's note: The impact on the UE and the IMS core with solution in clause 8.6 (Media Tunnelling Solution) is FFS.

Editor's notes: Separate tables should be created to discuss impact on the core network and impact on the packet core.

10.1.2 Impact on IMS core

Table 10.1.2: Summary of impact of various candidate solutions on the IMS core

Solution	Characteristics	Impact on the IMS core
8.2 Tunnelling solutions transparent to the existing IMS core	Tunnel endpoint (TEP) on the IMS core side and UE	One of the main goal of this solution is to remain transparent to the IMS core.
8.3 Reuse of Existing TLS solutions	Additional requirements on the UE, P-CSCF, and TURN server	Since this solution make use of all the existing protocols in the IMS world, there is no impact on the IMS core
8.4 Tunnelled services control function (TSCF)	New network element TSCF is introduced	Given the fact that TSCF function makes use of the authentication services and other security features provided by the IMS core, there is no impact to the existing IMS core.
8.5 Reuse of IKE/IPSEC	Enhance the security gateway (SEG) operations and similar enhancements for ePDG	This solution modified IPSEC and IKE to run over TCP on the ePDG and hence there is no impact to the IMS core.

10.1.3 Impact on packet core

Table 10.1.3: Summary of impact of various candidate solutions on the packet core

Solution	Characteristics	Impact on the packet core
8.2 Tunnelling solutions transparent to the existing IMS core	Tunnel endpoint (TEP) on the IMS core side and UE	Since the Tunnel is terminated in the IMS core, there is no impact in the packet core since for the packet core these packets looks like regular IP packet.
8.3 Reuse of Existing TLS solutions	Additional requirements on the UE, P-CSCF, and TURN server	Since this solution makes use of all the existing protocols in the IMS world, there is no impact on the packet core.
8.4 Tunnelled services control function (TSCF)	New network element TSCF is introduced	With the TSCF, since the tunnel is terminated in the IMS network in the case of iFire, there is no impact in the packet core.
8.5 Reuse of IKE/IPSEC	Enhance the security gateway (SEG) operations and similar enhancements for ePDG	This solution modified IPSEC and IKE to run over TCP on the ePDG and hence there could be impact in the packet core.

10.2 Co-existence with other NAT/FW traversal solution for IMS

Table 10.2: Summary on impact of candidate solutions co-existing with other NAT/FW traversal solution for IMS. (The existing firewall traversal mechanisms in 3GPP are ICE/STUN/TURN and IPSec/IKEv2)

Solution	Characteristics	Co-existence with other IMS traversal solutions
8.2 Tunnelling solutions transparent to the existing IMS core	Tunnel endpoint (TEP) on the IMS core side and UE	This solution first checks whether the firewall traversal mechanism has to be invoked. The assumption at this stage is that all the existing firewall traversal mechanism has failed.
8.3 Reuse of Existing TLS solutions	Additional requirements on the UE, P-CSCF, and TURN server	Since this solution make use of all the existing protocols in the IMS world, this solution can co-exist with other IMS traversal mechanism
8.4 Tunnelled services control function (TSCF)	New network element TSCF is introduced	Given the fact that the TSCF mechanism is invoked only when all the existing firewall traversal mechanism in the IMS world fails, the TSCF mechanism can co-exist with other IMS traversal mechanisms.
8.5 Reuse of IKE/IPSEC	Enhance the security gateway (SEG) operations and similar enhancements for ePDG	Given the fact that the IKE/IPSEC mechanism is invoked only when all the existing firewall traversal mechanism in the IMS world fails, the IKE/IPSEC mechanism can co-exist with other IMS traversal mechanisms

11 Conclusions and recommendations

For fixed terminals, current trends and interop events shows that support of ICE/STUN etc. are becoming commonly supported. Furthermore WebRTC mandates usage of ICE/STUN. The conclusion is therefore that for fixed terminals, it is more likely that these would adopt minor addition to ICE/STUN procedures (with support of HTTP CONNECT), than a new tunneling protocol.

For mobile or dual mode terminals, FS_FIRE and SMURFs are largely overlapping. Most of the functionality in the ePDG is needed for SMURFs, but currently the ePDG does not support the use of TCP based tunneling. To meet early RCS deployment needs, a solution for FS_FIRE (similar to the TSCF solution) which could run as a part of P-CSCF or ePDG is prioritized for specification over SMURF. This solution may prioritize a limited set of tunneling functionalities (for example, it will reuse the authentication mechanism at the IMS level), required for UE accessing IMS services through restrictive firewalls.

The following is concluded:

- The extensions (HTTP CONNECT and detection mechanism for determining firewall types and explicit mention of supporting TCP port 443) to STUN/TURN/ICE shall be standardized.

- The tunnelling interface for the SMURFs solution shall be terminated by a functional entity offering some of the functionality currently offered by an ePDG (e.g. IP address allocation), but use TCP (setup with HTTP CONNECT), use port 80 and 443, and look like HTTP/HTTPS. The interfaces of this tunnelling endpoint towards the core networks shall be identical, as far as possible, to the current interfaces between an ePDG and the core network for SMURFs. In order to meet early RCS deployment needs, the subset of SMURFs functionality required for UE accessing IMS services through restrictive firewalls (e.g., IP allocation) is prioritized for specification.

Editor's Note: Other solutions or extension to existing traversal mechanisms should be considered in the future

Annex A:
TSCF protocol overview

NOTE: This is an example on how TSCF tunnelling protocol could look like.
However, it is up to 3GPP WG CT1 to decide on the Stage 3 details of the protocol.

A.1 Control Message (CM) structure

A.1.1 Introduction

The Control Packets/Messages, denoted as CM in the pressent document, is used to exchange configuration information between TSE and TSCF. Control Messages (CMs) are of type REQUEST/RESPONSE.
The CM RESPONSE to a REQUEST MUST include either a corresponding REPLY or an error code indicating why the request could not be honored.

Control Messages utilize a simple TLV (Type Length Value) encoding with the packet format as described below

0										1										2										3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
TLV Type								TLV Length (8 bits)								TLV Value …																**Octet 1-4**
TLV Value [until Length is reached]...																																

A TLV is defined as the variable length concatenation of a unique Type (represented by an integer) and a Value containing the actual value identified by the Type.

A.1.2 General message structure and encoding rules

Integer/binary values must be encoded in network byte order. ASCII strings must be Null terminated except where explicitly specified. All Control Messages must include Control Message Header (CM_header) at the beginning of every Control Message (CM_header is explained in the next clause).

Control Message header MAYBE followed by TLVs.

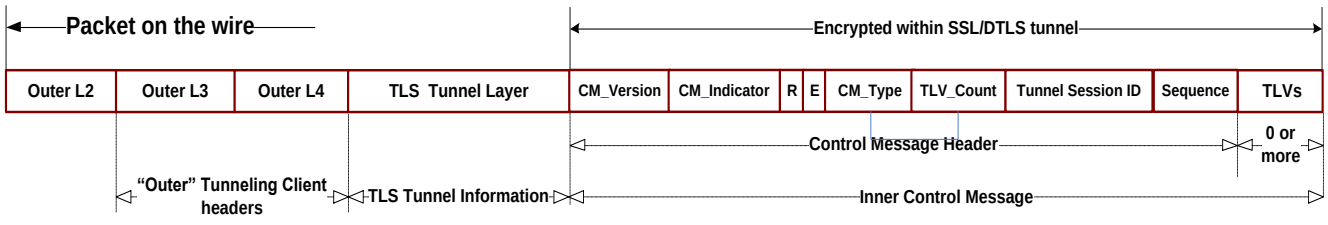


Figure A.1.2: Control Message structure

A.1.3 Control Message header

All Control Messages include Control Message Header (CM_header) at the beginning of the Control Message. The format of the CM_header is as given below:

0										1										2										3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	
CM_Version				CM_Indication		R				CM_Type						TLV_Count																**Octet 1-4**
Tunnel Session ID																																**Octet 5-8**
Tunnel Session ID																																**Octet 9-12**
Sequence																																**Octet 13-16**
Optional TLVs																																

Table A.1.3 below describes various fields of the CM_header

Table A.1.3: Control Message header fields

Field Name	Semantics	Value Type	Length	Notes
CM_Version	Identifies version of this Header. 1 is Currently supported	Unsigned integer	4 bits	It is the firts nibble (4bits) of the first byte. Current version = 1 Versions 4 and 6 reserved for IP payload differentiation. (The first nibble of the first byte of IP header is the IP header version which is 4 for IPv4 and 6 for IPv6).
CM_Indication	Identifies whether the message is a control message or not	bits	2 bits	Must be set as 0 to indicate this is a CM message
Reserved	Must be set with 0	bits	2 bits	Must be set as 0
CM_Type	Identifies the type of Control Message. Refer to table below for a listing of Control Message Types	Unsigned integer	1 byte	See table below for a list of supported types.
TLV_Count	Indicates the number of TLVs that follow (or are appended to) this header in the current Control Message.	Unsigned integer	2 bytes	Please note that CM_header itself is not a TLV.
Tunnel Session ID	It is assigned by TSCF and uniquely identifies the TLS Tunnel	Unsigned integer	8 bytes	This is the session id to uniquely identify a tunnel session.
Sequence	An ever incrementing transaction counter.	Unsigned integer	4 bytes	Each outstanding REQUSET will contain a unique value

A.1.4 Tunnel Session ID (TSID)

Tunnel Session ID (TSID) is assigned by TSCF to uniquely identify a TLS tunnels.

The first [tunnel] configuration message has Tunnel Session ID (TSID) header field bits set to 1s (FFFF…).

The first response contains TSCF assigned TSID. After that, all following messages must contain the assigned TSID in their header. Messages that do not have the expected TSID must be dropped and the TLS tunnel should be terminated.

A.1.5 Control Message TLV types

Editor's notes: This clause does not cover the authentication mechanisms for TLS tunnel. The possible authentication mechanisms are for further study.

Table A.1.5-1 below enumerates Control Message TLV types and their description.

Table A.1.5-1: TLV types

TLV type		Semantics	Short (8 bits)/ Long (16 bits) Format	Value type	Length	Optional	Notes
Name	Value						
Reserved	0-2		Short		Any	n/a	
Response_Code	3	Used by response messages	Short	Unsigned integer	2 bytes	No	Not optional in responses.
Internal_IPv4_Address	4	IP Address (IPv4)	Short	Octet string	4 bytes	Yes	IPv4 support is mandatory
Internal_IPv4_Netmask	5	IP Address Mask (IPv4)	Short	Octet string	4 bytes	Yes	The internal network's netmask. It MUST be used only with an Internal_IPv4_Adress attribute.
Keep_Alive_Interval	6	Indicates to client an expected Keep Alive frequency in seconds. "0" value means that no Keep Alive Messages required.	Short	Unsigned integer	2 bytes	Yes	TSCF to TSE
Padding	8	Used to pad messages to desirable offset	Short	Octet string	Any	Yes	Used for aligning messages to the word boundary
Internal_IPv6_Address	18	IP Address (IPv6)	Short	Octet string	16 bytes	Yes	IPv6 Address
Internal_IPv6_Netmask	19	IP Address Mask (IPv6)	Short	Octet string	16 bytes		The internal network's netmask. It MUST be used only with an Internal_IPv6_Adress attribute.
Reserved	23-255		Short (8 bit)	-	-	-	Reserved for future use

Table A.1.5-2 below gives the value for the response code. Every CM request must be responded back with a CM response which must have one of the following response code TLV.

Table A.1.5-2: Response_Code TLV

Name	Value	Semantics	Notes
Success	0	This message type will include requested configuration information request	
Invalid tunnel session ID	1	The value of the Tunnel Id is invalid	
Source IP address is blacklisted	2	The source IP address is not a valid IP address	
Out of tunnel resources	3	Maximum number of tunnels reached	
Service Unavailable	4	Service Unavailable	
Version_Not_Supported	5	Invalid version	
Reserved	7~255		

A.1.6 Configuration_Request message

The Configuration_Request message allows the TSE to obtain configuration information from the TSCF for the TLS tunnel. Tables A.1.6-1/2 below list the CM_Header values as well as required and optional TLVs that may be contained in a *Configuration_Request* message.

Table A.1.6-1: Configuration_Request CM_Header

Field Name	Value	Notes
Version_ID	1	Current = 1
CM_Indication	0	Must be set as 0 to indicate this is a CM message
Reserved	0	Must be set as 0
CM_Type	1	=*Configuration_Request*
TLV_Count	variable	This excludes the CM_Header itself
Session ID	variable	Session ID is assigned by TSCF to uniquely identify the TLS Tunnel
Sequence	variable	Sequence number for the message

Table A.1.6-2: Configuration_Request TLVs

TLV Name	Order	Value	Optional	Notes
Internal_IPv4_Address	n/a	IPv4	No	
Internal_IPv4_Netmask	n/a	IPv4	No	255.255.255.255 is the most common case
Internal_IPv6_Address	n/a	IPv6	Yes	
Internal_IPv6_Netmask	n/a	IPv6	Yes	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF is the most common case
Keep_Alive_Interval	n/a		Yes	

Tables A.1.6-3/4 below list CM_Header values as well as required and optional TLVs that may be contained in a RESPONSE to *Configuration_Request* message:

Table A.1.6-3: Configuration_Response CM_Header

Field Name	Value	Notes
Version_ID	1	Current = 1
CM_Indication	0	Must be set as 0 to indicate this is a CM message
Reserved	0	Must be set as 0
CM_Type	2	=*Configuration_Response*
TLV_Count	variable	This excludes the CM_Header itself
Session ID	variable	Session ID is assigned by TSCF to uniquely identify the TLS Tunnel
Sequence	variable	Response always has the corresponding Request sequence number.

Table A.1.6-4: Configuration_Response TLVs

TLV Name	Order	Value	Optional	Notes
Response_Code	1	Status Code		
Internal_IPv4_Address	n/a	IPv4	No	
Internal_IPv4_Netmask	n/a	IPv4	No	
Internal_IPv6_Address	n/a	IPv6	Yes	
Internal_IPv6_Netmask	n/a	IPv6	Yes	FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF is the most common case
Keep_Alive_Interval	n/a		Yes	

A.1.7 Configuration_Release_Request Message

Configuration_Release_Request Message can be used to graciously terminate a tunnel.
The response to Configuration_Release_Request must be Configuration_Release_Response message.
Table A.1.7-1 below lists the *CM_Header* values in a *Configuration_Release_Request* message. No TLV is contained in the *Configuration_Release_Request*.

CM_Header:

Table A.1.7-1: Configuration_Release_Request CM_Header

Field Name	Value	Notes
Version_ID	1	Current = 1
CM_Indication	0	Must be set as 0 to indicate this is a CM message
Reserved	0	Must be set as 0
CM_Type	5	=*Configuration_Release_Request*
TLV_Count	0	No TLV
Session ID	variable	Session ID must be same as initial Configuration_Request
Sequence	variable	Request Sequence number

Tables A.1.7-2/3 below list *CM_Header* values as well as required and optional TLVs that may be contained in a RESPONSE to *Configuration_Release_Request* message: *Configuration_Release_Response*.

The CM_header for the Configuration_Release_Response message is given in Table A.1.7-2 below.

Table A.1.7-2: Configuration_Release_Response CM_Header

Field Name	Value	Notes
Version_ID	1	Current = 1
CM_Indication	0	Must be set as 0 to indicate this is a CM message
Reserved	0	Must be set as 0
CM_Type	6	=*Configuration_Release_Response*
TLV_Count	1	Response_Code
Session ID	variable	Session ID is same as the Configuration_Release_Request
Sequence	variable	Response always has the corresponding Request sequence number.

Table A.1.7-3: Configuration_Release_Response TLVs

TLV Name	Order	Value	Optional	Notes
Response_Code	1	Status Code		

A.1.8 Keep Alive mechanism

In order to maintain pin-holes in a Firewall the Tunneling Client and the TSCF may exchange Keep Alive Messages (Request/Response pairs) on preconfigured time interval. TLS tunnel Keep Alive Message (KAM) must always be sent within each maintained TLS tunnel if keep alive mechanism is negotiated through the configuration messages.

NOTE: Keep Alive Messages (KAMs) could be sent in absence of "real" traffic.
In other words, KAMs could be sent/exchanged only during silence/no activity periods.

Table A.1.8-1: KAM request CM_Header

Field Name	Value	Notes
Version_ID	1	Current = 1
CM_Indication	0	Must be set as 0 to indicate this is a CM message
Reserved	0	Must be set as 0
E	0	Current = 0, no extension defined
CM_Type	7	=*Keep_Alive*
TLV_Count	0	No Additional TLVs in KAM
Session ID	variable	Session ID must be same as initial Configuration_Request
Sequence	variable	Request Sequence number

There will be no additional TLVs associated with KAM message.

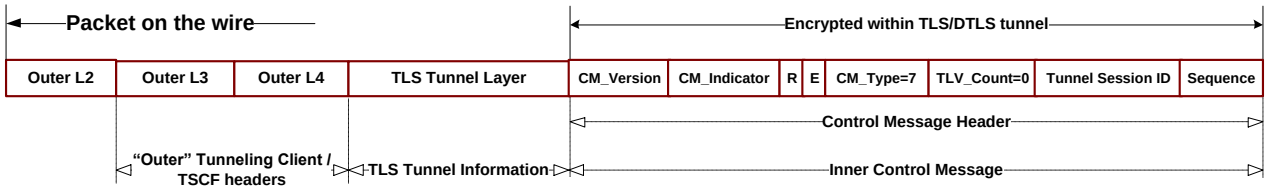


Figure A.1.8: Keep_Alive request Message structure

Table A.1.8-2 below lists CM_Header values as well as required and optional TLVs that may be contained in a RESPONSE to *Keep_Alive* message: *Keep_Alive_Response*

Table A.1.8-2: Keep_Alive_Response CM_Header

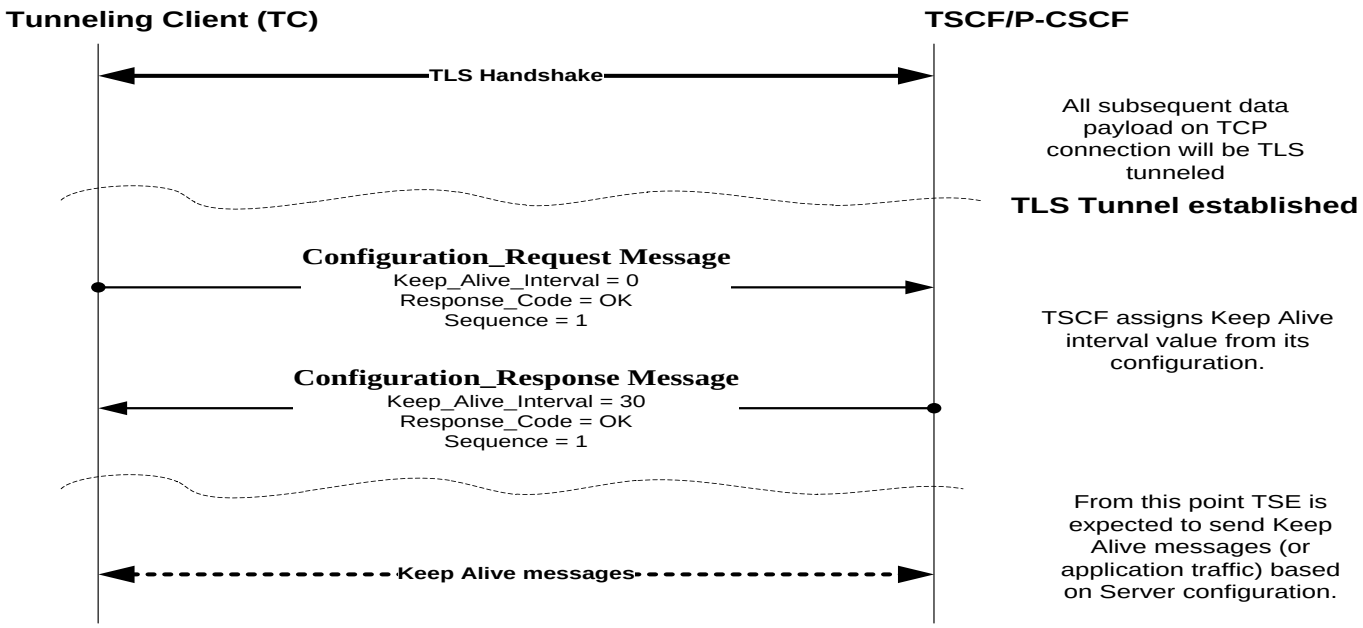
Field Name	Value	Notes
Version_ID	1	Current = 1
CM_Indication	0	Must be set as 0 to indicate this is a CM message
Reserved	0	Must be set as 0
CM_Type	8	=*Keep_Alive_Response*
TLV_Count	0	No additional TLVs in KAM response
Session ID	variable	Session ID must be same as initial Configuration_Request
Sequence	variable	Same as Request Sequence number

After TLS tunnel establishment, TSCF function will expect (if explicitly configured) to receive a Keep Alive Message (KAM) from TSE periodically on pre-determined time interval. If KAM is not received as expected, TSCF function will terminate the tunnel. If TSCF function receives KAM, it will respond with Keep Alive Response of it is own toward TSE. The response will contain the same sequence as a Client's REQUEST. If TSE does not receive KAM as expected, TSE should terminate the tunnel. The KAM time interval could be explicitly configured on TSCF and TSE in which case TSCF and TSE does not have to use the configuration messages to communicate the KAM interval.

A.1.8.1 Keep Alive time Interval assignment by TSCF

The TSCF may optionally assign a Keep Alive message Interval from its configuration.

The message flow below enables TSCF to configure TSE with Keep Alive Interval:



A.1.9 Inner IP address assignment by TSCF

The TSCF assigns an inner IP address to TSE as a part of the TLS tunnel establishment.

This addressis used as an "inner" source address by TSE in all communications to TSCF.
TSCF could obtain the inner IP address from the 3GPP AAA server, could be configured locally on the TSCF server or by other means.

The message flow Figure A.1.9 below enables TSCF to configure TSE with inner IP address/mask:

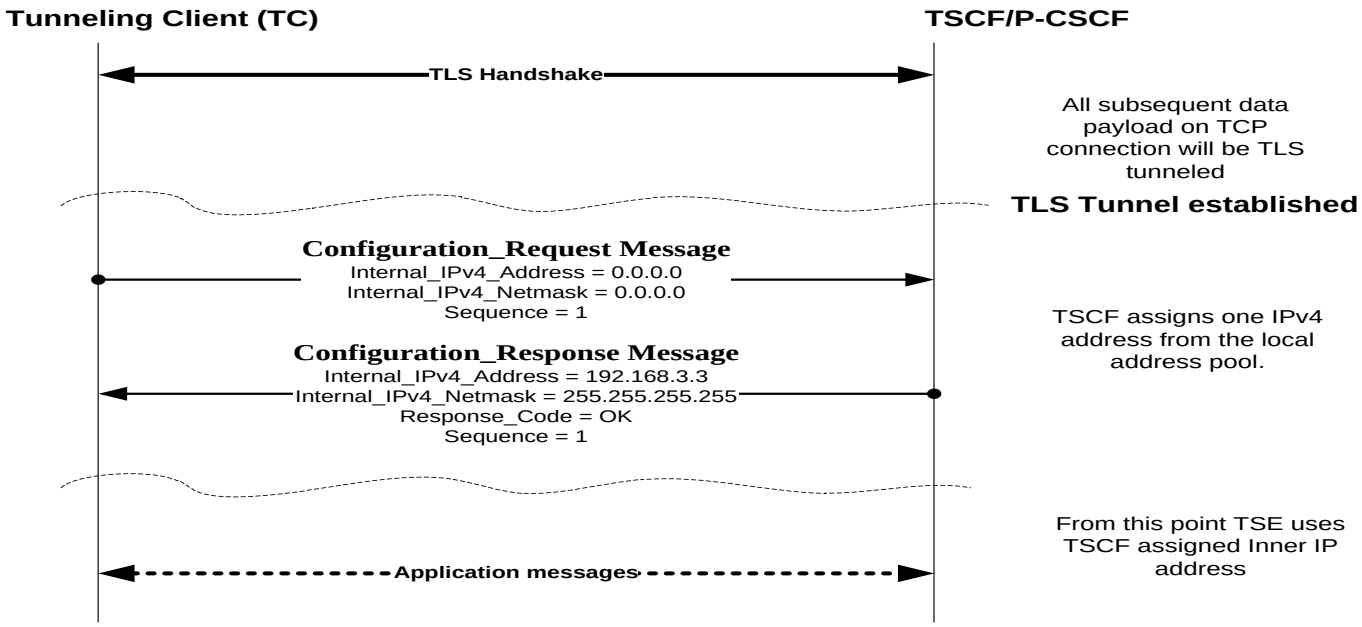


Figure A.1.9: Inner IP Address Assignment Message Flow

Annex B:
Change history

Change history							
Date	**TSG #**	**TSG Doc.**	**CR**	**Rev**	**Subject/Comment**	**Old**	**New**
2011-11	SA3#64		-	-	Editor's Initial Draft	-	0.1.1
2012-02	SA3#66		-	-	Changes indicated by change marks	-	0.1.2
2012-05	SA3#67		-	-	Changes indicated by change marks	-	0.1.4
2012-07	SA3#68		-	-	Changes indicated by change marks	-	0.2.0
2012-11	SA3#69		-	-	Changes indicated by change marks	-	0.2.1
2012-11	SA3#70		-	-	Changes indicated by change marks	-	0.3.0
2013-04	SA3#71		-	-	Changes indicated by change marks	-	0.3.1
2013-07	SA3#72	S3-130869	-	-	Changes indicated by change marks	-	0.4.0
2013-09	-	-	-	-	MCC clean-up	0.4.0	0.4.1