Use Cases for Session-Specific Session Initiation Protocol (SIP) Session Policies
draft-hilt-sipping-policy-usecases-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 8, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This draft describes use cases for session-specific Session Initiation Protocol (SIP) sessions policies.
Table of Contents

1. Introduction ............................................. 3
2. Use Cases ................................................. 3
   2.1  Media Intermediary .................................... 3
       2.1.1  General Overview ................................ 3
       2.1.2  Traffic Monitoring ............................... 7
       2.1.3  Enforcing SLA/Access Control .................... 7
       2.1.4  Load Balancing and Traffic Shaping ............... 7
       2.1.5  QoS Marking ..................................... 8
       2.1.6  NAT/Firewall Traversal ......................... 8
       2.1.7  Media-level Topology Hiding ..................... 8
       2.1.8  IPv4/IPv6 Interworking .......................... 8
       2.1.9  Media Encryption ................................ 9
   2.2  Limitations and Restrictions ....................... 9
       2.2.1  General Overview ................................ 9
       2.2.2  Limit Bandwidth ................................ 10
       2.2.3  Restrict Codec Usage ............................ 11
       2.2.4  Restrict Media Type Usage ...................... 11
3. Security Considerations ................................. 12
4. IANA Considerations .................................... 12
5. Informative References ................................ 12
   Authors' Addresses ........................................ 13
   Intellectual Property and Copyright Statements ....... 14
1. Introduction

Some domains have policies in place, which impact the sessions established using the Session Initiation Protocol (SIP) [3]. These policies are often needed to support the network infrastructure or for the execution of services. For example, wireless networks usually have limited resources for media traffic. A wireless network provider may want to restrict codec usage on the network to lower rate codecs or disallow the use of high bandwidth media types such as video.

Session policies provide a mechanism for a network domain to communicate these policies to user agents. With session policies, user agents know about the policies in the network and can adjust their sessions so that they comply with these policies or simply connect to a domain with less stringent policies.

There has been much discussion in the IETF about the most suitable protocol for session-specific Session Initiation Protocol (SIP) policies [2]. The goal of this draft is to describe common use cases in which session-specific policies are expected to be used. Particularly controversial in this discussion is the mechanism for conveying session information from the user agent to the policy server. This draft will therefore describe the session information a policy server needs to know for each of the discussed use case scenarios.

This document focuses on session-specific policies. In some of the use cases it might also be possible to use session-independent policies [1]. However, session-independent policies are outside of the scope of this document and their use will not be discussed here.

2. Use Cases

Most of the use cases for session-specific policies are based on the insertion of a media intermediary or the limitation of certain aspects of a session. The two categories of use cases are discussed separately in the sections below.

2.1 Media Intermediary

This section provides a general overview over the insertion of a media intermediary with session policies. It then discusses use cases that are based on intermediaries.

2.1.1 General Overview

In this scenario it is assumed that a UA A is located in a policy
enabled domain (see Figure 1), which has an outbound proxy (P A), a policy server (PS A) and a media intermediary (M A). UA A places a call to a UA in another domain (UA B).

--- SIP Signaling
=== Policy Channel
*** Media

Figure 1

In step (1) in Figure 2 UA A sends out an INVITE and receives the address of the policy server PS A in step (2). It discloses session information (from the offer) to policy server PS A in step (3). The information disclosed includes the IP address and port (b) UA A is going to use for inbound streams.

The policy server uses this information to create an address binding for inbound media streams on M A. The binding connects a port on M A (port (a) in Figure 2) to the address and port provided by UA A (i.e. port (b)). With this binding, M A forwards all incoming traffic on port (a) to port (b) on UA A.

UA A must use the address of M A and port (a) in the offer (instead of its own address and port). PS A therefore returns the policy shown in Figure 3 to UA A in step (4). This policy contains the address of M A (192.0.2.0) and port (a) (6000/6001). Using this policy, UA A creates a new offer' and sends it to UA B in step (5). UA B will now send its media to port (a) on M A. From there it will be forwarded to port (a) on UA A. Thus, M A has been inserted into the inbound media stream.

UA A receives an answer in step (6) and discloses the address of UA B and port (d) (extracted from the answer) to the policy server PS A in step (7). PS A sets up a second binding now for outbound streams on the M A. This binding connects port (c) on M A to the address and port that was in the answer (i.e. the address of UA B and port(d)).
The address of MA and port (c) is returned to UA A in a policy in step (8). UA A applies this policy to the answer. Thus, UA A will now send its outbound traffic to MA, which in turn forwards it to UA B. MA has also been inserted into the outbound media stream.

Proxy PA stays in the signaling path and removes the address bindings on MA when the session is terminated.

Media streams can be encrypted by the UAs. In many cases, media intermediaries need to decrypt the encrypted streams. UA A may therefore need to provide an intermediary with the encryption keys for the current session.

Information the UA needs to disclose to the policy server on the policy channel:

- **offer**: the UA discloses the IP addresses and ports of all media streams in the offer. The UA may also need to disclose the encryption keys used for the current session.
- **answer**: the UA discloses the IP addresses and ports of all media streams in the answer. The UA may also need to disclose the encryption keys used for the current session.
In the above call flow, intermediaries are inserted by modifying the address and ports of media streams. Other techniques for inserting a media intermediary such as using IP tunneling or TURN are also feasible but not discussed in this draft.
2.1.2 Traffic Monitoring

Traffic monitoring generally requires that an entity in the network can examine the media packets of a flow. It may also require that media streams can be associated with SIP sessions.

A media intermediary that has been inserted into a media stream as described above can examine media packets as required. Media streams can be associated with the session for which the policy was created.

2.1.3 Enforcing SLA/Access Control

It is often desirable to enforce policies on media streams, for example, according to a Service Level Agreement (SLA). Enforcing policies requires that a network entity can monitor traffic and, in case policies are violated, block traffic as needed.

Traffic monitoring can be performed by a media intermediary. The intermediary can also decide whether packets are compliant to a given policy or not. It can block streams if policies are violated by dropping the respective packets.

An intermediary can enforce many types of media-level policies. For example, it can enforce limitations session aspects (e.g., codecs, bandwidth, media types), ensure that the media streams correspond with what has been announced in the session description and it can reject traffic that is sent outside of a SIP session. The intermediary can also terminate streams for other reasons, for example, if the user runs out of credit.

2.1.4 Load Balancing and Traffic Shaping

Load balancing and traffic shaping typically requires that the network can determine the route of media streams independent of the path that would be chosen by IP routing. This type of route selection can take multiple criteria into account such as current traffic conditions or peering agreements. For example, a service provide may be connected to another service provider through two links and may want to selectively route calls over one or the other link. In another example, a service provide wants to route traffic through a domain that would otherwise not be traversed by the media streams.

A media intermediary can perform traffic shaping and load balancing. The intermediary receives packets from the UA and can determine the next hop destination for these packets.

A service provider may have multiple media intermediaries at
strategic locations in the network. By selecting one of these intermediaries for a session, it forces the corresponding media streams to go through the chosen intermediary. This way, media traffic can be directed through a specific link, to a certain part of the network or through a certain domain. The routing decision is made by simply including a specific intermediary into the path.

### 2.1.5 QoS Marking

Two approaches for QoS marking on media streams are feasible with session policies:

- **Hosted QoS marking:** A media intermediary is inserted as described above. The intermediary performs QoS marking.
- **Endsystem-based QoS marking:** The policy server returns a session policy that contains the desired DSCP value (following the flow described in Section 2.2). The endpoint itself performs QoS marking using this DSCP value.

### 2.1.6 NAT/Firewall Traversal

NAT/firewall traversal requires that the NAT/firewall is inserted into the media path. Each endpoint sends its traffic to the NAT/firewall, which then forwards it to the destination on the other side of the NAT/firewall as permitted by NAT/firewall policies.

An media intermediary that is inserted into the media path as described above can act as NAT/firewall.

### 2.1.7 Media-level Topology Hiding

Topology hiding is mostly done at the signaling level. However, media-level topology may be used to hide the addresses of media endpoints inside the network.

A media intermediary inserted into streams as described above can perform media-level topology hiding. Such a media intermediary will usually act as RTP mixer/translator. It can remove all internal IP addresses and possibly other sensitive information carried in RTCP reports.

### 2.1.8 IPv4/IPv6 Interworking

IPv4/v6 translation on media streams can also be performed by a media intermediary.
2.1.9 Media Encryption

A media intermediary can encrypt/decrypt media traffic before forwarding it. Media encryption/decryption requires that the intermediary has the encryption keys for the current session.

Media intermediaries may also need to decrypt encrypted media streams in order to perform other functionalities that require a deep inspection of RTP packets.

2.2 Limitations and Restrictions

This section provides a general overview over the use of session policies to restrict certain aspects of a session. It provides example use cases for some of these policies.

2.2.1 General Overview

The scenario is similar to Figure 1 except that there is no media intermediary (in a real architecture, it may still be present to perform other functionalities such as policy enforcement).

Steps (1) to (3) in Figure 4 are the same as above (see Figure 2).

After receiving offer information in step (3), the policy server determines whether a policy is needed or not. If a policy is needed, it is returned to UA A in step (4) (see policy examples below). The UA A creates a modified offer according to the received policies (step (5)) and completes the session setup in step (6).

Policies that define limitations or restrictions reduce available choices for session parameters. These policies only need to be applied to an offer because the answer can't extend the choices available in an offer.

The policy server PS A can asynchronously update the policy provided to UA A during session setup. For example, a policy server may wish to disallow a codec that was allowed by the initial session policy. In step (7) PS A sends an updated policy to UA A. This policy requires a change in the current session. UA A therefore updates the session by sending a re-INVITE with a modified offer in step (8).

The information the UA needs to disclose to the policy server depends on the individual use case and are described below.
2.2.2 Limit Bandwidth

In some environments there is only a limited bandwidth available to each user agent (e.g. in a wireless network). Communicating bandwidth limitations to the user agent enables the user agent to make an informed decisions, for example, about the codecs or media types to be used in a session.
The following example policy informs the UA of a 80 kbit/s bandwidth limit. In the context of session-specific policies, this policy is returned if the offer can result in a session that exceeds the allowed maximum bandwidth. The offer that is created based on this policy should not contain choices that may exceed the maximum bandwidth (e.g. it could consist of one audio stream and the codecs G.711 and G.729).

```xml
<session-policy>
  <max-bandwidth>80</max-bandwidth>
</session-policy>
```

Information the UA needs to disclose to the policy server about the offer on the policy channel:

- The UA must disclose all aspects of a session that may affect the media bandwidth used. These are typically the number of streams together with the media type and the codecs available on a stream. Alternatively, the UA can disclose a maximum bandwidth value.

### 2.2.3 Restrict Codec Usage

Networks may want to impose restrictions on the codecs that can be used. With session-specific policies it is possible to tell the UA that some of the codecs in the offer are prohibited.

The following example policy informs the UA that the codecs G.729 and G.723 are not allowed. Offer should therefore not include G.729 and G.723.

```xml
<session-policy>
  <codecs default-policy="allow">
    <codec policy="disallow">G729</codec>
    <codec policy="disallow">G723</codec>
  </codecs>
</session-policy>
```

Information the UA needs to disclose to the policy server about the offer on the policy channel:

- The UA must disclose all codecs it has included in the offer.

### 2.2.4 Restrict Media Type Usage

Similar to codecs, it is possible to restrict the use of media types using session-specific policies.
The example policy below defines that audio is required, video is allowed and all other media types are disallowed.

```
<session-policy>
  <media-types default-policy="disallow">
    <media-type policy="mandatory">audio</media-type>
    <media-type policy="allow">video</media-type>
  </media-types>
</session-policy>
```

Information the UA needs to disclose to the policy server about the offer on the policy channel:

- The UA must disclose all media types it has included in the offer.

3. Security Considerations

This draft describes the use of mechanisms defined in other drafts and does not introduce additional security issues.

4. IANA Considerations

This draft does not introduce new identifiers or namespaces.

5. Informative References


Authors' Addresses

Volker Hilt
Bell Labs/Lucent Technologies
101 Crawfords Corner Rd
Holmdel, NJ 07733
USA

Email: volkerh@bell-labs.com

Gonzalo Camarillo
Ericsson
Hirsalantie 11
Jorvas 02420
Finland

Email: Gonzalo.Camarillo@ericsson.com
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The Internet Society (2005). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.