Network Working Group	B. Stucker	
Internet-Draft	Nortel	
Intended status: Informational	H. Tschofenig	
Expires: May 15, 2008	Nokia Siemens Networks	
	November 12, 2007	

TOC

Analysis of Middlebox Interactions for Signaling Protocol Communication along the Media Path
draft-sipping-stucker-media-path-middleboxes-00

Status of this Memo

Abstract

Middleboxes are defined as any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host. Two such functions are network address translation and firewalling.
When Application Layer Gateways, such as SIP entities, interact with NATs and firewalls, as described in the MIDCOM architecture, then problems may occur in the transport of media traffic when signaling protocol interaction takes place along the media path, as it is the case for recent key exchange proposals (such as DTLS-SRTP). This document highlights problems that may arise. Unfortunately, it is difficult for the end points to detect or predict problematic behavior

and to determine whether the media path is reliably available for packet exchange.
This document aims to summarize the various sources and effects of NAT and firewall control, the reasons that they exist, and possible means of improving their behavior to allow protocols that rely upon signaling along the media path to operate effectively.

Table of Contents

---

1. Introduction

TOC

According to by RFC 3234 [RFC3234] (Carpenter, B. and S. Brim, “Middleboxes: Taxonomy and Issues,” February 2002.) middleboxes are defined as any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host.
In the context of SIP a SIP ALG may interact with a node along the media path to control network address translation, firewalling, and other functions.

> With firewall control packet filters are installed based on the SIP signaling interaction to implement a behavior of 'deny by default' in order to reduce the risk of unwanted traffic. This function is often referred to as 'gating'. Depending on the timing of the packet filter installation and the content of the packet filter signaling traffic along the media, such as DTLS-SRTP or ICE, may be treated in an unexpected way.
>
> In cases where the middlebox is involved in overcoming unmanaged NAT traversal the case is similar. The key feature of this type of NAT traversal is a desire to overcome the possible lack of information about any [RFC4787] (Audet, F. and C. Jennings, “Network Address Translation (NAT) Behavioral Requirements for Unicast UDP,” January 2007.) address and/or port mapping by a possibly unknown NAT device (server reflexive address and filtering properties). In particular, a NAT binding for an endpoint may not exist yet for the address and port identified in the endpoint's SDP. As such, a pilot packet sent by that endpoint behind the NAT is required to create the necessary mappings in the NAT for the media relay to deliver media destined for that endpoint. Until that pilot packet is received no media packets may be reliably forwarded to the endpoint by the relay.

This document presents a summary of these two techniques, discusses their impact upon other protocols such as ICE and DTLS-SRTP, and proposes a set of recommendations to mitigate the effects of gating and latching on in-band negotiation mechanisms.

---

2. Terminology

TOC

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.).
We use the terms filter, policy action (or action), policy rule(s), MIDCOM agent, and MIDCOM Policy Decision Point (PDP) as defined in [RFC3303] (Srisuresh, P., Kuthan, J., Rosenberg, J., Molitor, A., and A. Rayhan, “Middlebox communication architecture and framework,” August 2002.). The MIDCOM agent is co-located with a SIP ALG that comunicates with the firewall or the media relay.

TOC

3. Architecture

Figure 1 (Analysed Firewalling Architecture) shows the architecture that is being considered in this document with respect to firewall and NAT traversal using media relaying. The timing and directionality with which media packets are allowed to traverse a particular edge device is the subject of this investigation. The MIDCOM agent thereby pushes policy rules to the middlebox that allow or deny certain flows to bypass. Additionally, in case of media relaying it is important for the MIDCOM agent to adjust the signaling messages.

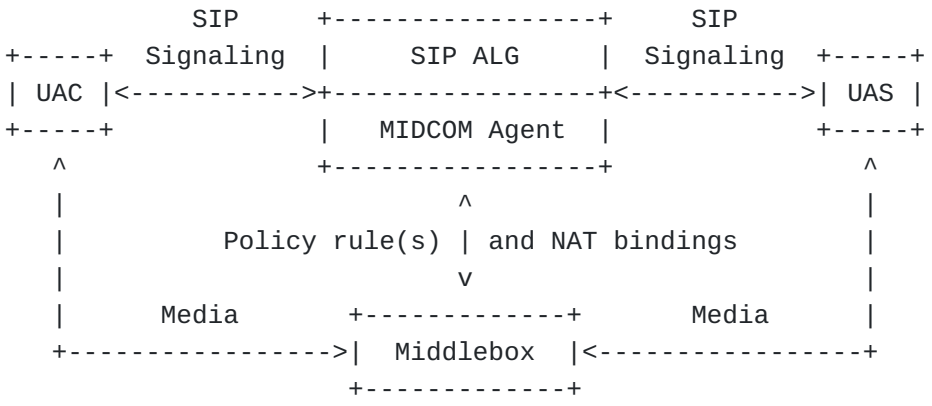

Figure 1: Analysed Firewalling Architecture

The aspects of packet filtering are described in Section 4 (Packet Filtering) whereas NAT traversal is illustrated in Section 5 (NAT Traversal).

4. Packet Filtering

TOC

Figure 1 (Analysed Firewalling Architecture) highlights the interaction between the MIDCOM agent and the middlebox. These two elements inspect call control signaling and media path packets and determine when packets from a given source to a given destination are allowed to flow between endpoints. It is common for the gate controller to be the local outbound proxy for a given SIP UA being gated.
The primary responsibility of the MIDCOM agent, which is co-located with a SIP entity, is to examine the call control signaling to determine the media addresses and ports used to define the media path between the gated device and the endpoint(s) with which it is

corresponding. For SIP, this would correspond to the media addresses described within SDP after at least one full offer/answer exchange. This information is used to create one or more packet filters that describe the expected media path(s) for the call. These packet filters are combined with an algorithmic determination, typically based on the state of the call, as to which direction(s) media packets are allowed to flow between the endpoints, if at all. The filter and the action that is being installed by the MIDCOM agent at the middlebox may change during the lifetime of a SIP signaling session, depending on the state of the call or on changes of the address and port information of one (or even both) of the end points.

It is possible that the gate controller may not be able to establish an exact address or port for one endpoint involved in the call in which case it may wildcard the address and/or port for the source and/or destination endpoint in the packet flow filter. In such a case, the packet flow filter is considered to have matched against a given media packet for the wildcarded field.

Note that it is possible to specify the filter using wildcards, for example, if some end point address information is not known at a given point in time. Additonally, the default firewalling policy is subject to local configuration ('deny per default' vs. 'permit per default'). For a given SIP signaling sessions the policy at the MIDCOM agent might be very strict with respect to the packets that are allowed to flow in a particular direction. For example, packets may be allowed to flow in both directions, only in one direction for a specific media stream. No particular behavior can be assumed.

When a media session is destroyed (end of call, deleted from the session description, etc.), the MIDCOM agent removes policy rules created for that media session at the middlebox.

4.1. Protocol Interaction

TOC

MIDCOM agents may employ a variety of models to determine when to change the status of a particular policy rule. This is especially true when a call is being established. For SIP, this would be when an early dialog is established between endpoints. Although there is the potential for a great deal of variability due to an intentional lack of specification, typically, one of two models is used by the MIDCOM agent to determine the state of a policy rule during call setup: single-stage and two-stage commit. The term 'commit' here refers to the point at which a policy rule is setup that allows media traffic to flow. For example, this would be the point at which packets for a media stream marked a=sendrecv in SDP was allowed to flow bi-directionally by the middlebox.

4.1.1. Single-Stage Commit

TOC

Single stage commit is commonly used when the MIDCOM agent is most involved only in firewalling. For SIP, MIDCOM agents use a single-stage commit model typically install policy rules for the call when the 200 OK to the INVITE is received in the case that the INVITE contained an SDP offer, or when the ACK is received if the initial offer was sent in the 200 OK itself.
This model is often used to prevent media from being sent end-to-end prior to the call being established.

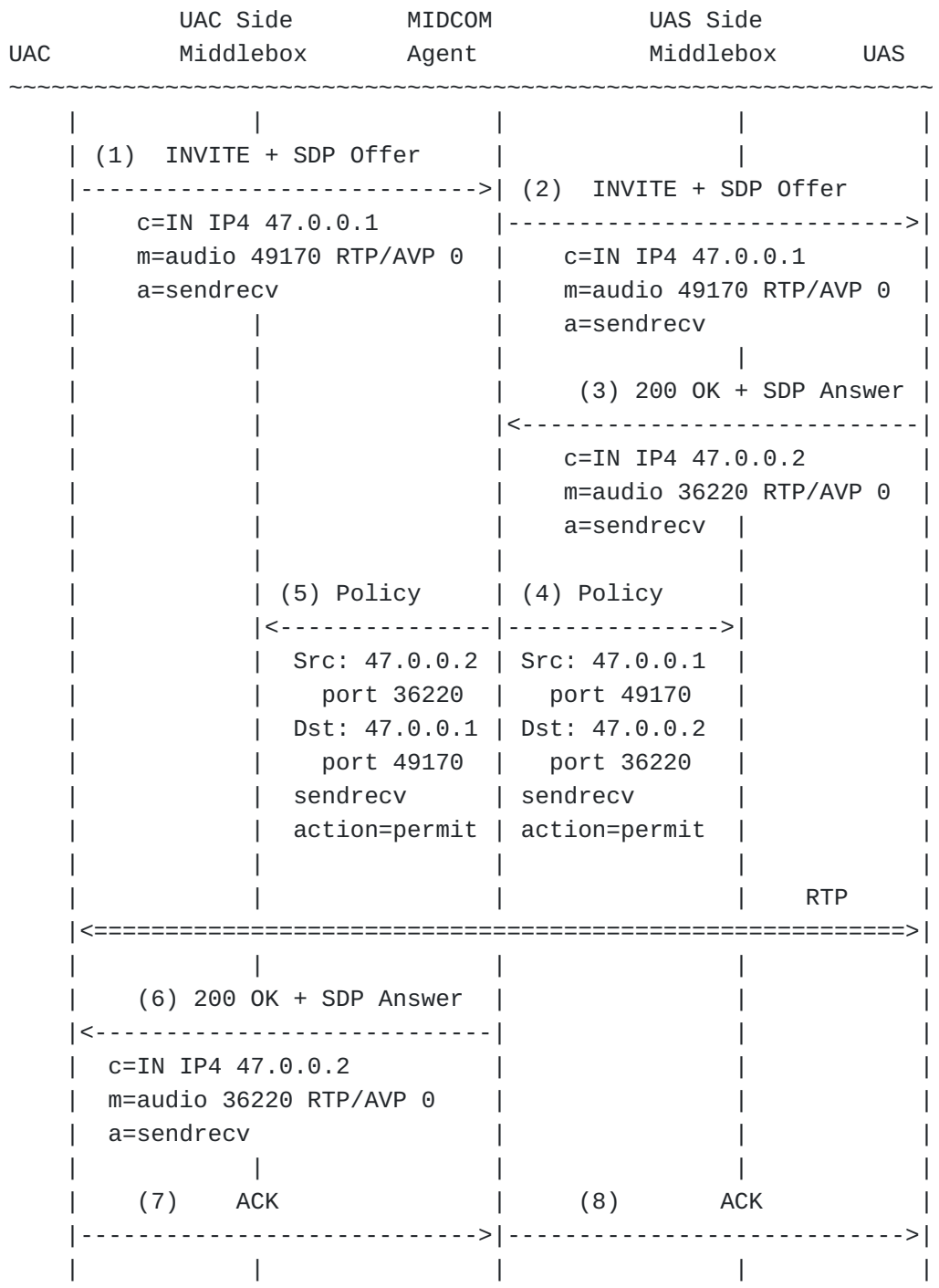

Figure 2: Example Single-stage Commit with SIP and SDP

In the example above, policy is created in steps 4 and 5 to allow bi-directional media flow based on the SDP exchanged in steps 1 and 3. In this example, the MIDCOM agent installes the policies after the 200 OK to the INVITE arrives in step 3. With a firewalling policy of 'deny by

default' media sent prior to steps 5 and 4 by the UAC or UAS is discarded by the middleboxes.
Noted that early media that arrives before the 200 OK would require special treatement since otherwise it would be dropped as well.

4.1.2. Two-Stage Commit

TOC

Two-stage commit is used when the MIDCOM agent also providers functionality, such as Quality of Service signaling that may require resources to reserved early on in the call establishment process before it is known if the call will be answered. An example of this would be where the MIDCOM agent is responsible for guaranteeing a minimum level of bandwidth along the media path. In this case an initial set of policies may be sent by the MIDCOM agent to the middlebox even though they are put into a pending state but trigger a resource reservation. Later, when the call is accepted, the gate controller may update the state of the policies to active them.

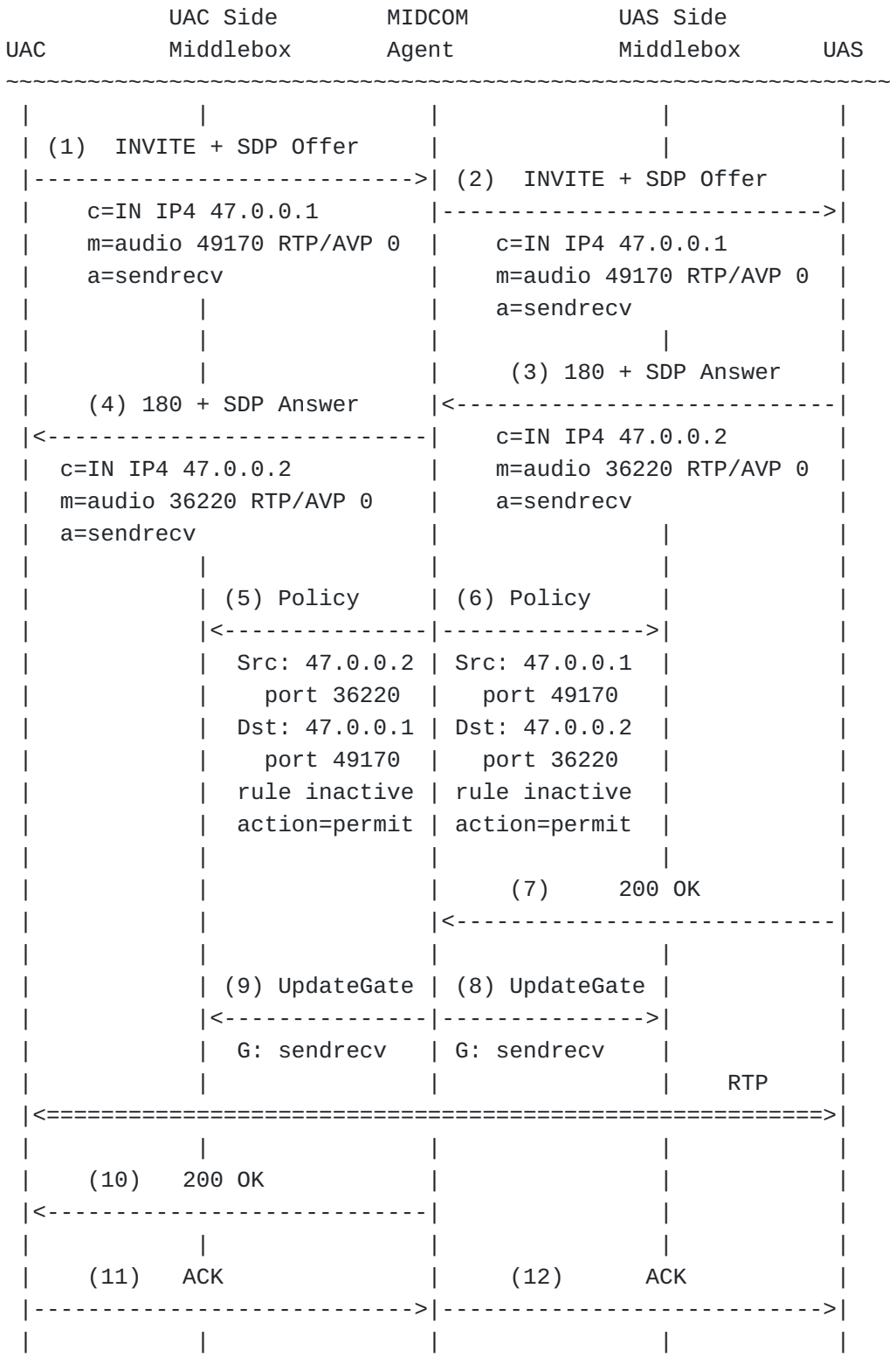

Figure 3: Example Two-stage Commit with SIP and SDP

In the example above, policies are created in steps 5 and 6 based off of the SDP sent in steps 1 and 3 in an initial inactive state (no packets are allowed to flow) despite the SDP indicating the media should be bi-directional. This interaction with the middlebox, however, triggers a QoS reservation to take place. Later, when the 200 OK to the INVITE comes in step 7, the policies are updated in steps 8 and 9 to indicate that packets should be allowed to flow bi-directionally. Although functionally equivalent to the single-stage commit example given earier in Figure 2 (Example Single-stage Commit with SIP and SDP), other operations at the gate agent may have been performed simultaneously in steps 5 and 6 that justifies the early explicit definition of the gates in an inactive state. The full usage of PRACK here is not shown for purposes of brevity.

4.2. Further Reading

TOC

Packet filtering based on the approach described in this document has been described in a number of documents. Although the usage of this architecture can also be found on the Internet their behavior is largely specified only in documents that relate to IMS standardization. The behavior of the devices deployed on the Internet is therefore largely undocumented. Nevertheless, the following documents give the reader a better idea of the functionality and the signaling interaction. These documents may also specify an additional behavior in relation to how packet filtering is used when the MIDCOM agent is responsible for processing SIP/SDP call control signaling and the middlebox is responsible for a variety of activities beyond pure filtering. For example, it is common for middleboxes to exempt RTCP flows from being blocked even though the associated RTP flows are not allowed to flow in order to support RTCP signaling while a call is on hold. These references are given here for the reader to gather a better understanding of how this is mechanism is used in various forums and is non-exhaustive:

1. 3GPP, "TS 23.203: Policy and charging control architecture" (3GPP, “Policy and charging control architecture,” September 2007.) [TS-23-203]

2. 3GPP, "TS 29.214: Policy and charging control over Rx reference point" (3GPP, “Policy and charging control over Rx reference point,” September 2007.) [TS-29-214]

3. ETSI TISPAN, "ES 282-003: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture" (ETSI, “Telecommunications and Internet converged Services and Protocols for Advanced

Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture," June 2006.)
[TISPAN-ES-282-003]

4. Cablelabs, "PacketCable 2.0: Quality of Service Specification (PKT-SP-QOS-I01-070925)" (CableLabs, "PacketCable 2.0: Quality of Service Specification," September 2007.)
[PKT-SP-QOS-I01-070925]

Note that different terms are used for the MIDCOM agent and the middlebox. For example, in an IMS context the MIDCOM agent would be part of the P-CSCF and PCRF elements or in TISPAN it would be part of the P-CSCF, A-RACF and SPDF that are involved in controlling gating operations. Many different elements perform the role of a middlebox: GSM GGSN, CDMA PDSN, SAE serving gateway, TISPAN A-BGF/C-BGF/I-BGF, PacketCable CMTS, etc. These functions may be present in the network in a unified or decomposed architecture.

---

5. NAT Traversal

TOC

One NAT traversal technique that is being used is based on media relay. As shown in Figure 1 (Analysed Firewalling Architecture) the MIDCOM agent that is being co-located with the SIP ALG functionality interacts with the middlebox that is also a NAT in order to request and allocate NAT bindings. A side effect of the interaction with a (double) NAT is that the media traffic is forced to traverse a certain NAT in both directions (also called media anchoring).
This architecture could be compared with a STUN relay [I-D.ietf-behave-turn] (Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," July 2009.) that is being controlled by the MIDCOM agent rather than the end point itself. The motivation why this technique is being used in favor to other NAT traversal techniques is that clients do not have to support anything beyond RFC 3261 [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) and network administrators can control and apply local policy to the relay binding process in a centralized manner.

5.1. Protocol Interaction

TOC

The MIDCOM agent's role is to inspect call control signaling and update media address and port values based upon media relay binding

information allocated with the middlebox/media relay. For SIP, this minimally involves updating the c= and m= lines in the SDP, although some implementations may update other elements of the SDP for various reasons.
Because the endpoints may not be able to gather a server reflexive address for their media streams, the MIDCOM agent employs the following algorithm to ensure that media can flow to the given endpoint:

1. Give the corresponding endpoint an address and port on the middlebox for them to send media to for the endpoint served by the MIDCOM agent.

2. Give the served endpoint a different address and/or port on the middlebox for it to send media to for the corresponding endpoint.

3. Use the address and port the corresponding endpoint supplies for media streams as the destination for packets sent to the middlebox by the served endpoint.

4. Use the address and port of the first packet received from the served endpoint at the middlebox as the destination for packets sent to the middlebox by the corresponding endpoint.

An example of this algorithm is shown in Figure 4 (Call Flow with SIP + SDP) using SIP and SDP. In this example the UAC is the endpoint served by the MIDCOM agent, which is also acting as a local outbound proxy, and the UAS is the corresponding endpoint.

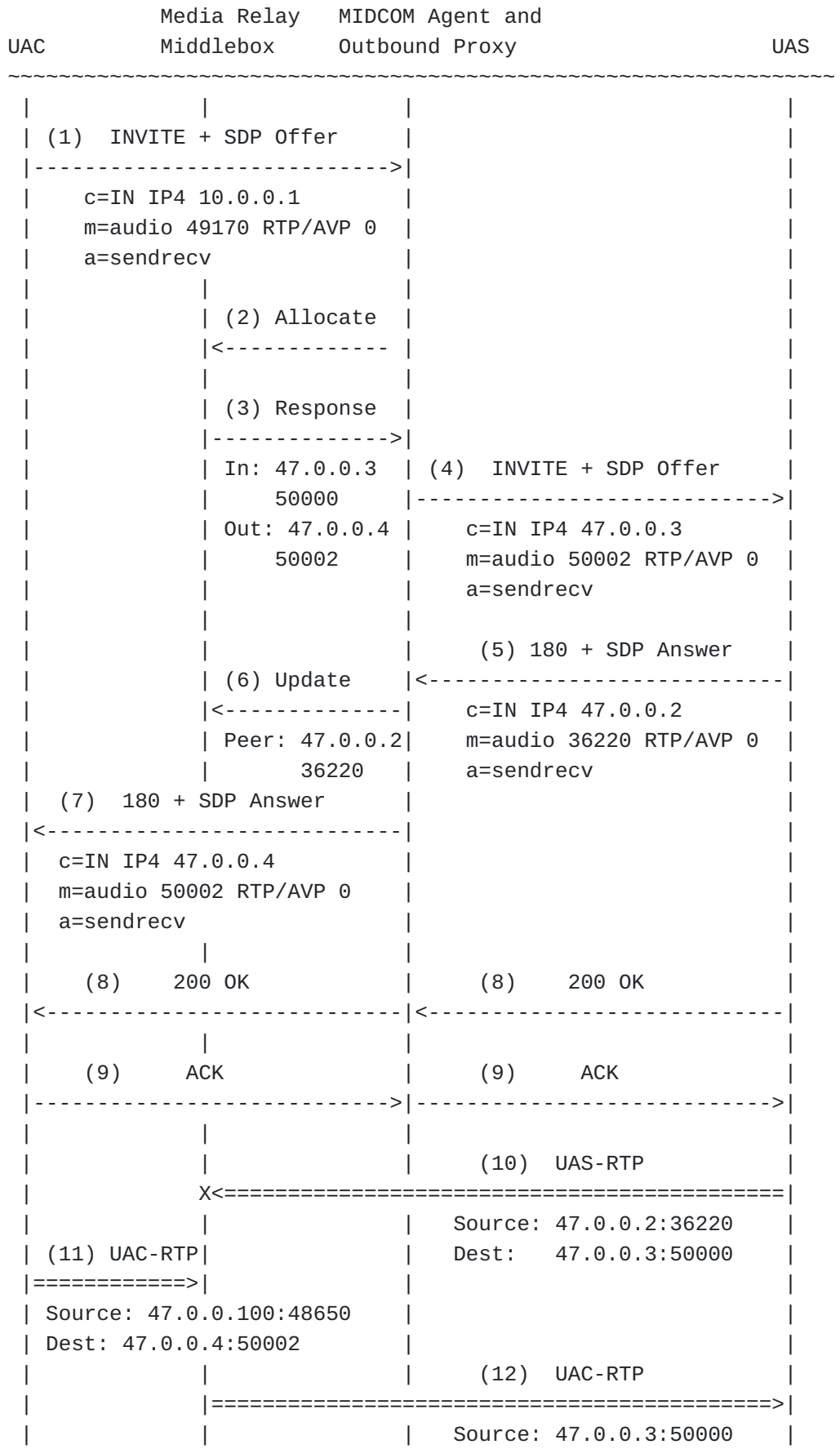
Media Relay
Middlebox
MIDCOM Agent and
Outbound Proxy
UAC
UAS
(1) INVITE + SDP Offer
c=IN IP4 10.0.0.1
m=audio 49170 RTP/AVP 0
a=sendrecv
(2) Allocate
(3) Response
In: 47.0.0.3
50000
Out: 47.0.0.4
50002
(4) INVITE + SDP Offer
c=IN IP4 47.0.0.3
m=audio 50002 RTP/AVP 0
a=sendrecv
(5) 180 + SDP Answer
c=IN IP4 47.0.0.2
m=audio 36220 RTP/AVP 0
a=sendrecv
(6) Update
Peer: 47.0.0.2
36220
(7) 180 + SDP Answer
c=IN IP4 47.0.0.4
m=audio 50002 RTP/AVP 0
a=sendrecv
(8) 200 OK
(8) 200 OK
(9) ACK
(9) ACK
(10) UAS-RTP
Source: 47.0.0.2:36220
Dest: 47.0.0.3:50000
(11) UAC-RTP
Source: 47.0.0.100:48650
Dest: 47.0.0.4:50002
(12) UAC-RTP
Source: 47.0.0.3:50000

Figure 4: Call Flow with SIP + SDP

---

1. UAC sends INVITE to local outbound proxy, which is also a MIDCOM agent, with an SDP offer.

2. The MIDCOM agent looks at the signaling and determines that a NAT may be present (Via header address mismatch with observed source address, etc.). It asks the middlebox to allocate a media relay binding.

3. The middlebox responds with a media relay binding that consists of an inbound address/port for media from the UAS, and an outbound address/port for media from the UAC.

4. The MIDCOM agent updates the addresses in the SDP offer with the inbound address/port information from the middlebox/media relay binding response.

5. The UAS responds with a 180 containing an SDP answer.

6. The MIDCOM agent interacts with the middlebox to update the destination address/port information from the SDP answer for media to be sent to the UAS, and changes the addresses/ports in the SDP answer to the UAC with the outbound address/port information from the middlebox binding from step 3. Media can now flow to the UAS from the UAC at the middlebox/media relay.

7. The UAC receives the SDP answer containing the media relay outbound address/port information.

8. The UAS answers the INVITE with a 200 OK.

9. The UAC acknowledges with an ACK.

10. RTP for the UAS (which may have begun flowing prior to answer) flows to the middlebox, but the middlebox has no reliable address to relay the media to for the UAC yet. Media will typically be dropped.

11. RTP arrives at the media relay on the inbound address/port from the UAC. The middlebox observes the source address and port of the arriving packet and completes the binding process. The

source address and port of the media from the UAC is now the destination address/port for media arriving on the outbound port of the middlebox/media relay from the UAS.

12. Media from the UAC is relayed to the UAS.

13. Media from the UAS is relayed to the UAC. It is up to local policy at the media relay as to whether or not packets that had arrived from the UAS for the UAC are queued or dropped prior to the UAC's address/port information being updated in step 11.

5.2. Further Reading

TOC

Although the described NAT traversal approach is used by a number of implementations to overcome incorrect address/port information in call control signaling from an endpoint behind a NAT, only one reference is known that describes the functionality in a standardized manner.

1. ETSI TISPAN, "ES 282-003: Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture" (ETSI, “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture,” June 2006.) [TISPAN-ES-282-003]. The TISPAN Ia interface between the TISPAN BGF and SPDF is the relevant specification.

---

6. Interactions between Media Path Signaling and Middlebox Behavior

TOC

This section points to the problems that occur when signaling exchanges are performed along the media path when middleboxes are present that behave in the way described in this document.

6.1. Firewalling

TOC

The description in Section 4 (Packet Filtering) highlighted that the timing of the policy rule installation by the MIDCOM agent towards the

middlebox has an impact on when and what media traffic is allowed to traverse.
Hence, the middlebox prevents the exchange of packets in the media path until the session establishment signaling has reached a pre-configured milestone where the MIDCOM agent signals to the middlebox that packets are allowed to traverse in both directions. Prior to this, packets may be allowed to flow uni-directionally to satisfy certain service requirements or may be entirely blocked by the middlebox. For SIP [RFC3261] (Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol," June 2002.) the typically milestone that must be reached is offer/answer exchange [RFC3264] (Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)," June 2002.) accompanied by an acknowledgement that the dialog has been accepted by the UAS (i.e., 200 OK to the INVITE). A concrete example of the impact can be found with the case of key exchange along the media path, as it is provided by DTLS-SRTP. Figure 2 of [I-D.fischl-sipping-media-dtls] (Fischl, J., "Datagram Transport Layer Security (DTLS) Protocol for Protection of Media Traffic Established with the Session Initiation Protocol," July 2007.) shows that the arrival of the SIP INVITE at the UAS triggers the DTLS handshake. This message would be blocked by the middlebox, as described in Section 4 (Packet Filtering) since the MIDCOM agent has not yet installed policy rules. The consequence is that the DTLS key exchange is delayed until the policy rules are installed and that media traffic that is sent before the DTLS exchange is completed may be dropped and the user experiences clippping.
Unlike with the pilot packet used for NAT traversal, the bi-directional media path is established via the signaling path, not via packets sent along the media path. In some deployment models, RTCP is always available bi-directionally regardless of the installed policy rules. Obviously, this is not a property that can be guaranteed to be true in the future.

6.2. NAT Traversal

TOC

The described NAT traversal interaction prevents asynchronous exchange of packets in the media path until a pilot packet has been received by the middlebox from the endpoint being served. It can be employed for both the [RFC3264] (Rosenberg, J. and H. Schulzrinne, "An Offer/Answer Model with Session Description Protocol (SDP)," June 2002.) offerer and/or answerer. Therefore, in the worst case, both endpoints must generate a pilot packet towards each other to ensure a bi-directional media path exists. Any signaling on the media path that relies upon a uni-directional handshake in the reverse direction may not complete until media in the forward direction by the other endpoint. If

signaling on the media path is required to complete prior to media generation the handshake may stall indefinitely.

---

7. Preliminary Recommendations

TOC

The following preliminary recommendations are suggested:

> **REC #1:** It is recommended that any protocol handshake on the media path ensure that a mechanism exists that causes both endpoints to send at least one packet in the forward direction as part of, or prior to, the handshake process. Retransmission of STUN connectivity checks (see [I-D.ietf-behave-rfc3489bis] (Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for (NAT) (STUN)," July 2008.)) as part of ICE [I-D.ietf-mmusic-ice] (Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," October 2007.) is an example of such a mechanism that satisfies this recommendation.
>
> **REC #2:** It is recommended that middleboxes present on the media path allow a nominal amount of traffic to be exchanged between endpoints to enable completion of media path signaling prior to the session being established. The amount of traffic necessary to complete the signaling between endpoints is expected to be orders of magnitude smaller than that of any sufficiently interesting fraudulent traffic.
>
> **REC #3:** It is recommended that failure to complete signaling on the media path not automatically cause the session establishment to fail unless explicitly specified by one or more endpoints. A fallback scenario where signaling on the media path is retried after the session has been established is recommended.

---

8. Security Considerations

TOC

This document talks about security related functionality and the impact of one security mechanism, namely firewalling, to another one, namely key management for media security.

TOC

9. IANA Considerations

This document does not require actions by IANA.

---

10. Acknowledgements

TOC

We would like to thank Steffen Fries, Dan Wing, Eric Rescorla, and Francois Audet for their input to this document. Furthermore, we would like to thank Jason Fischl, Guenther Horn, Thomas Belling, Jari Arkko, Cullen Jennings for the discussion input to this problem space.

---

11. References

TOC

11.1. Normative References

TOC

[RFC2119]	Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC3261]	Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, “SIP: Session Initiation Protocol,” RFC 3261, June 2002 (TXT).
[RFC3264]	Rosenberg, J. and H. Schulzrinne, “An Offer/Answer Model with Session Description Protocol (SDP),” RFC 3264, June 2002 (TXT).
[RFC3303]	Srisuresh, P., Kuthan, J., Rosenberg, J., Molitor, A., and A. Rayhan, “Middlebox communication architecture and framework,” RFC 3303, August 2002 (TXT).

11.2. Informative References

TOC

[I-D.fischl-sipping-media-dtls]	Fischl, J., "Datagram Transport Layer Security (DTLS) Protocol for Protection of Media Traffic Established with the Session Initiation Protocol," draft-fischl-sipping-media-dtls-03 (work in progress), July 2007 (TXT).
[I-D.ietf-behave-rfc3489bis]	Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for (NAT) (STUN)," draft-ietf-behave-rfc3489bis-18 (work in progress), July 2008 (TXT).
[I-D.ietf-behave-turn]	Rosenberg, J., Mahy, R., and P. Matthews, "Traversal Using Relays around NAT (TURN): Relay Extensions to Session Traversal Utilities for NAT (STUN)," draft-ietf-behave-turn-16 (work in progress), July 2009 (TXT).
[I-D.ietf-mmusic-ice]	Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols," draft-ietf-mmusic-ice-19 (work in progress), October 2007 (TXT).
[PKT-SP-QOS-I01-070925]	CableLabs, "PacketCable 2.0: Quality of Service Specification," September 2007.
[RFC3234]	Carpenter, B. and S. Brim, "Middleboxes: Taxonomy and Issues," RFC 3234, February 2002 (TXT).
[RFC4347]	Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security," RFC 4347, April 2006 (TXT).
[RFC4787]	Audet, F. and C. Jennings, "Network Address Translation (NAT) Behavioral Requirements for Unicast UDP," BCP 127, RFC 4787, January 2007 (TXT).
[TISPAN-ES-282-003]	ETSI, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Resource and Admission Control Sub-system (RACS); Functional Architecture," June 2006.
[TS-23-203]	3GPP, "Policy and charging control architecture," September 2007.
[TS-29-214]	3GPP, "Policy and charging control over Rx reference point," September 2007.

Authors' Addresses

TOC

	Brian Stucker
	Nortel
	2201 Lakeside
	Richardson, TX 75082

	USA
Email:	bstucker@nortel.com
URI:	http://www.linkedin.com/in/bstucker
	Hannes Tschofenig
	Nokia Siemens Networks
	Otto-Hahn-Ring 6
	Munich, Bavaria 81739
	Germany
Email:	Hannes.Tschofenig@nsn.com
URI:	http://www.tschofenig.com

Full Copyright Statement

TOC

Intellectual Property