HIPRG
Internet-Draft
Intended status: Informational
Expires: April 26, 2007

H. Tschofenig
M. Shanmugam
Siemens Networks GmbH & Co KG

October 23, 2006

Traversing HIP-aware NATs and Firewalls: Problem Statement and Requirements

draft-tschofenig-hiprg-hip-natfw-traversal-05.txt

Status of this Memo

Copyright Notice

Abstract

The Host Identity Protocol (HIP) is a signaling protocol, which supports mobility and multihoming by adding a new layer in the TCP/IP stack. By carring relevant parameters in the signaling messages, HIP can be used to establish IPsec encapsulating security payload (ESP) security associations between two hosts. Middleboxes (e.g. firewalls and network address translators) cannot inspect transport layer headers of data traffic if that traffic is sent over an IPsec ESP tunnel. However, HIP is designed to be middlebox friendly; it enables the middleboxes to inspect the signaling messages. The information that they can derive from that messages enables the middleboxes to uniquely identify the subsequent data flows, e.g. for the purposes of multiplexing and demultiplexing . A middlebox that implements the relevant mechanisms is called "HIP-aware". This document presents a problem statement and lists some requirements that are necessary for a HIP-aware middlebox traversal technique. These include authentication and authorization of signaling end-hosts by the middleboxes. Such authorization will help the middleboxes to decide whether or not an end host is allowed to traverse, and can potentially limit unwanted traffic.

Table of Contents

1. Introduction

In the current Internet architecture, an IP address is used to locate and to identify a host, termed as "locator" and "identifier" respectively. Hosts that move and change their IP addresses are said to be mobile and those that prefer to be addressed with multiple IPs at a given time are said to be multihomed. Mobility and Multihoming are together expressed as Multiaddressing. When hosts use IP addresses for communication, all transport connections are bound to it. Changes to IP addresses mean breaking the existing transport bindings and establishing a new transport connection. Hence, the existing dual role of IP addresses are not able to cope with the requirements for multiaddressing.

The Host Identity Protocol (HIP) [I-D.ietf-hip-base], a multiaddressing proposal, presents a novel approach to separate the "identifier" role from the "locator" role by adding an additional layer between the traditional transport layer and the network layer. The transport layer uses a new, mobility-unrelated identifier called as Host Identity Tags (HITs), in place of IP addresses, while the network layer uses conventional IP addresses for routing. As the transport connections are bound to the HITs, they are not disturbed with the change in IP address. In other words, a host despite being mobile can use a single transport layer connection associated to one HIT and multiple IP addresses.

HIP uses a two-way handshake mechanism, termed as base exchange messages, to authenticate and to establish a connection with an end host. HIP also offers the functionality to carry IPsec ESP relevant

payloads together with the base exchange messages in order to establish IPsec ESP security associations, which are subsequently used to encrypt the data traffic between the two end hosts. Consequently, if HIP is used to establish IPsec ESP SAs then it will also inherit some of the well-known incompatibilities similar to IPsec ESP-NAT problems, as described in [RFC3715]. To overcome that, HIP allows the middleboxes to participate in the base exchange, inspect the relevant traffic identifiers and later the middleboxes will use those identifiers to distinguish and to allow a particular data traffic.

This document presents a problem statement in the context of HIP and middlebox traversal, and discusses the requirements that has to be addressed by a HIP-aware NAT/FW traversal technique.

[Editor's Note: The problem statement for the HIP dealing with legacy NATs is described in [I-D.irtf-hiprg-nat].]

The document is organized as follows: Section 3 presents the problem

statement, Section 4 sketches the overview of the HIP base exchange together with the middleboxes, Section 5 discusses possible scenarios and Section 6 discusses the requirements and properties for a HIP-aware middlebox solution.

2. Terminology

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].

This draft used the terminology defined in [RFC2663], [I-D.ietf-hip-base], [I-D.ietf-hip-esp] and [RFC4423] and [RFC2401].

The term SPI refers to the Security Parameter Index value used in IPsec packets. The initiator selects one SPI(I) that can be found in the ESP_info parameter, which is then used by the responder to create an IPsec packet (ESP packet in this case) for traffic sent to the initiator. The responder selects one SPI(R)(using ESP_info(R) parameter) which is used by the initiator to encrypt all data sent to

the responder.

Other relevant abbreviations can be found in [I-D.ietf-hip-base] and [I-D.ietf-hip-esp].

The concept of a flow identifier is described in [RFC4080].

We use the following notation throughout this document:

[x] indicates that x is optional.

{x} indicates that x is encrypted.

<x>y indicates that "x" is encrypted with the key "y".

--> signifies "Initiator to Responder" communication (requests).

<-- signifies "Responder to Initiator" communication (replies).

3. Problem Statement

Besides the communicating hosts in the Internet, the entities such as NATs and Firewalls play a major role in the event of delivering packets to an appropriate host, and each meant for specific functionality. For instance, NATs are used to combat the IPv4 address depletion problem, and Firewalls are erected to protect unsolicited information flowing in and out of a corporate network.

Typically, NATs use <src IP ,dst IP, src port, dst port, protocol> as a flow identifier to identify a particular traffic or connection. Because of this, protocols like IPsec suffers from well-known NAT related problems [RFC3715] (middleboxes cannot inspect the port numbers, when the packets are IPsec-ESP protected). To work around IPsec-NAT problems several approaches have been discussed, e.g., the NAT traversal approaches described in [RFC3947] and [RFC4306] allows the end hosts to detect one or more NATs in between them and [RFC3948] proposes to use the UDP encapsulation of IPsec ESP packets to traverse NATs.

If HIP uses IPsec protection for the data traffic then the flow identifier will take the shape of <destination IP address, SPI and ESP> in order to facilitate the middlebox traversal. Note that the flow identifier used here is one possible example and used throughout the document, however it could be possible to have other variants of flow identitier as well. Although HIP is described as a two-party protocol, middle boxes are supposed to intercept the base exchange messages to learn the flow identifier and to process them correctly. In other words, a multi party protocol is created such that the flow identifier is available to middle boxes between the HIP hosts. To achieve this, HIP aims to interact with middleboxes actively whereby these devices need to understand the HIP protocol and they need to be involved in the protocol exchange.

This interaction, obviously, requires the middleboxes to verify the authenticity of the base exchange messages in order to learn the flow identifier and to create a state i.e., NAT binding or a pinhole. In this context, to provide proper security, middleboxes should not be vulnerable to denial of service attacks and might want to authenticate or authorize entities before creating state information. Note that the IPsec SA is unidirectional and therefore two IPsec SAs (with two different SPIs, ESP_info contains the SPI value) have to be established.

Additionally, End hosts behind middleboxes, especially NATs, require the following steps to facilitate its reachability.

1. Connection, end host connects to the server, while doing that it

may also identify the middleboxes.

2. Registration, end host registers with the middlebox in order to inform the middlebox to relay its traffic.

3. Keep-alive, end host maintains the NAT registration by sending heart-beat messages.

4. Messaging, end host receives the solicited traffic.

HIP hosts can also make use of such procedures by binding their HITs (static identifier) with the middlebox to be connected, anywhere. Evidently, this requires the HIP hosts to perform a explicit registration mechanism with the middleboxes.

HIP also provides a way to deal with legacy NATs, as described in [I-D.nikander-hip-path]. To support this functionality, it is necessary to provide UDP encapsulation for both HIP signaling and IPsec packets. Legacy NAT traversal does not require NATs to be HIP aware or to understand the HIP message exchange.

4. HIP with Middleboxes

This section describes some sample message exchanges between the Initiator and the Responder, in which some of them situated behind a middlebox. Curently, this document explains the interaction of middlebox with plain HIP base exchange and the HIP base exchange carrying ESP payloads. However, this draft can also be extended to support other mechanisms.

4.1. HIP Base Exchange with middleboxes

Assume that the initiator starts the HIP base exchange, Figure 1 shows the HIP base exchange traversing a middlebox. Note that if a host wants to be contacted by the other peers, it needs some other mechanisms to signal its public address to the peers and, if necessary, should also inform the middlebox to allow the peers.

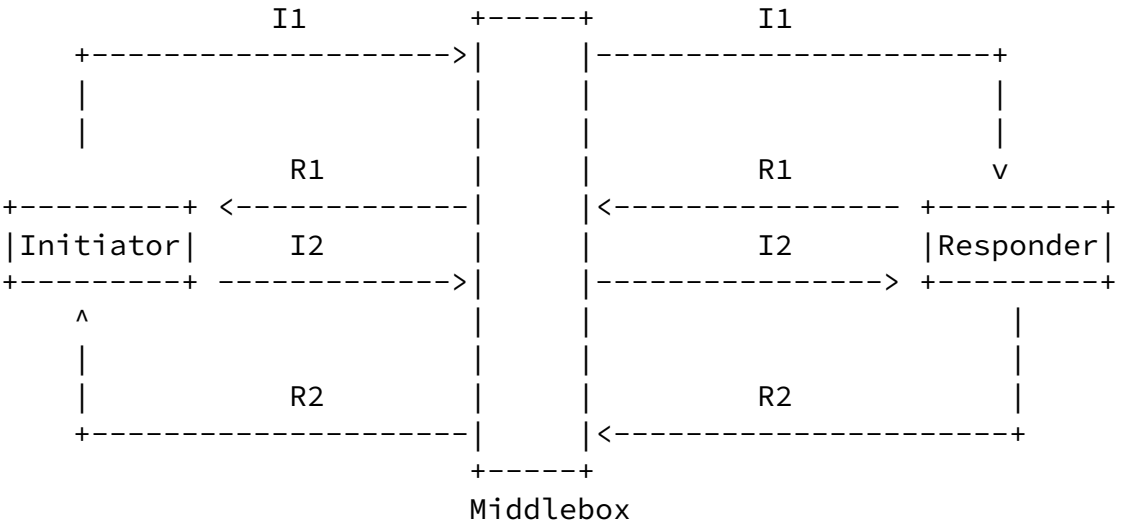


Figure 1: HIP Base Exchange and middleboxes

Subsequently, the HIP base exchange is depicted in more detail.

```
I -> R: I1: Trigger exchange

I <- R: R1: (Puzzle, {D-H(R), HI(R), HIP Transform})SIG

I -> R: I2: {Solution, LSI(I),D-H(I),
             HIP Transform, {H(I)}SK }SIG

I <- R: R2: {LSI(R), HMAC}SIG
```

Here, the base exchange becomes vulnerable to a DoS attack (for the

middleboxes) because the initiator's HI is encrypted in the I2 packet and the middleboxes are unable to verify the I2 message. As a consequence, an attacker may send spoofed I2 messages before the authentic initiator does that.

When HIP is used with HIP-aware NAT devices, the checksum, computed over the source and destination address, in the IP header must be recomputed. Additionally, it might be necessary to include support for storing the respective HITs and host identities.

4.2. HIP Base Exchange with ESP Parameters and Middleboxes

This section explains the HIP base exchange, carrying ESP parameters, together with the middleboxes and describes how the middleboxes may behave during the base exchange. Figure 3 shows the corresponding message exchange traversing a middlebox.

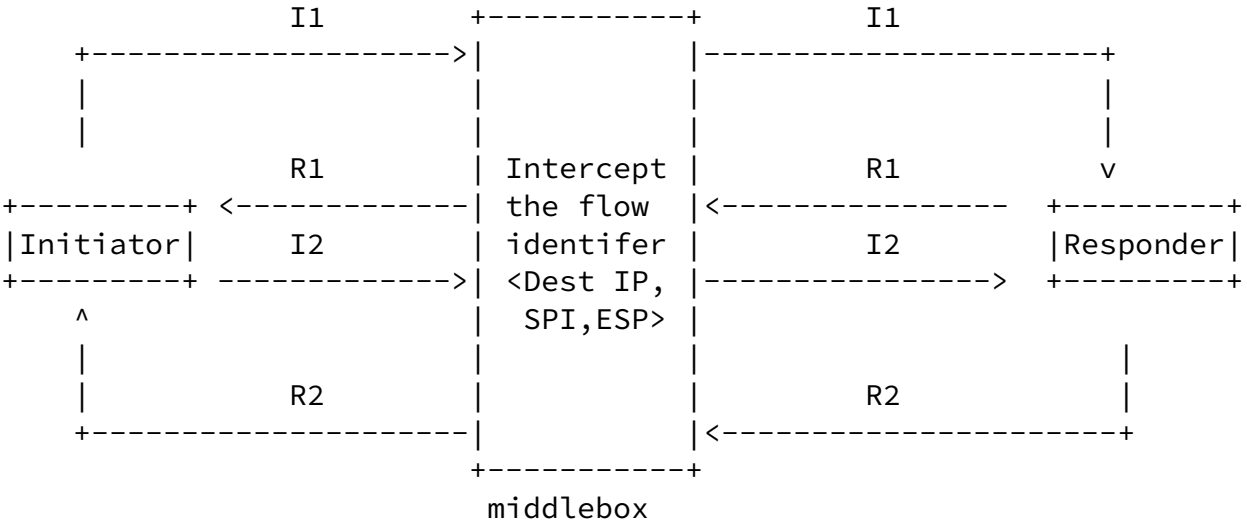


Figure 3: ESP Transport Format with HIP Base Exchange and Middleboxes

Subsequently, the HIP with ESP exchange is described in more detail.

I -> R: I1: Trigger exchange

```
I <- R: R1: {Puzzle, D-H(R), HI(R), ESP Transform,
             HIP Transform }SIG

I -> R: I2: {Solution, LSI(I), ESP_info(I), D-H(I),
             ESP_Transform, HIP Transform, {H(I)}SK }SIG

I <- R: R2: {LSI(R), ESP_info(R), HMAC}SIG
```


A potential responsibility of the middlebox, as shown in Figure 3, can be the following

- Intercept the signaling messages
- Authenticate and authorize the HIP nodes by verifying the signatures.
- Process the flow identifier information
- Perform actions according to the state machine
- Create state based on the content of message I2 with ESP_info(I) and R2 with ESP_info(R). Additionally, it might be necessary to include support for storing the respective HITs and host identities.

The middleboxes should participate in the signaling messages and has to learn the flow identifier to pass the subsequent data traffic.

Here, together with the spoofed I2 message, an attacker may send a bogus SPI value, which will result in an inconsistent state at NAT/FW.

4.3. HIP Mobility/Multihoming Exchange with Middleboxes

This section explains the HIP mobility and multihoming extensions for the HIP hosts [I-D.ietf-hip-mm] together with the middleboxes. Assume that the initiator moves after the base exchange and wants to inform the responder. During this procedure, the Initiator wants to start the rekeying procedure in order to establish new keys. Figure 5 shows the mobility message exchange, traversing a middlebox.

Note that this draft explains only one possible exchange for mobility, [I-D.ietf-hip-mm] provides a detailed message exchange for other variants such as rekeying initiated by responder.

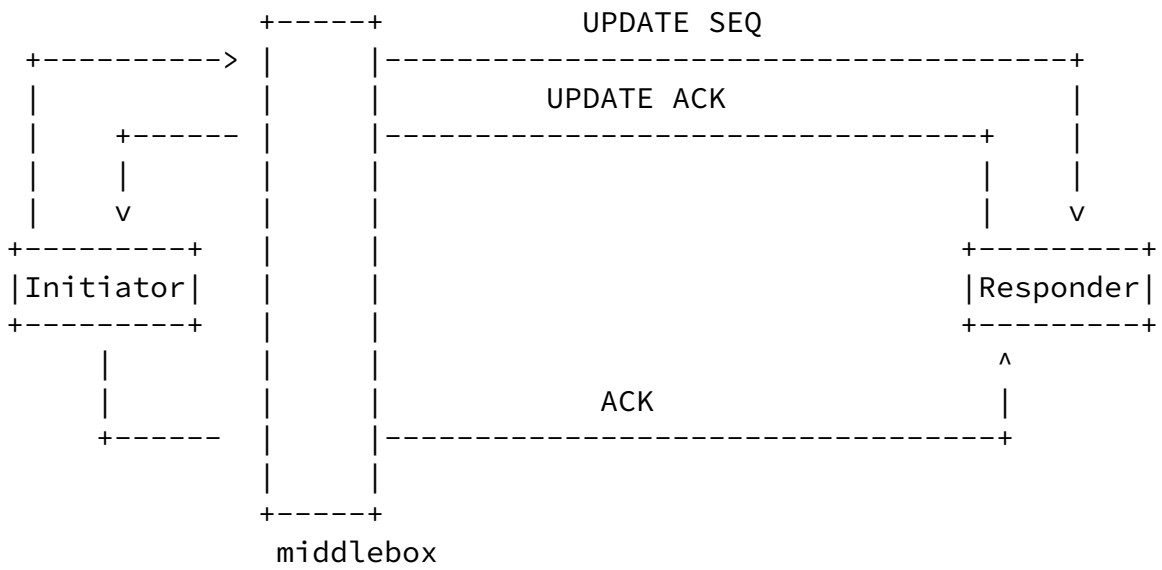


Figure 5: HIP Mobility Exchange with Middleboxee

Subsequently, the HIP mobility exchange is depicted below.

I -> R:UPDATE SEQ (ESP_INFO(I), LOCATOR, [DIFFIE_HELLMAN], SEQ)

I <- R:UPDATE ACK (ESP_INFO(R), SEQ, ACK,
[DIFFIE_HELLMAN], ECHO_REQUEST)

I -> R:ACK (ACK, ECHO_RESPONSE)

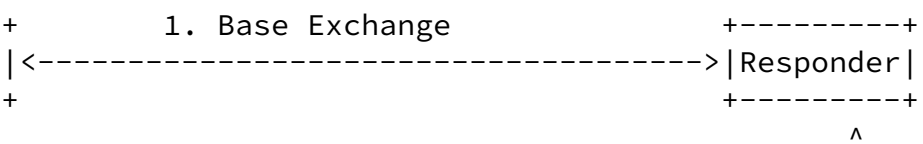
In such cases, a middlebox should,

- Intercept the HIP mobility messages
- Authenticate and authorize the HIP nodes by verifying the signatures
- Process the flow identifier information and perform actions according to the state machine
- Update the location of the initiator based on the "LOCATOR parameter" in the UPDATE messages, also in case of rekeying, the middlebox should update the state based on the information in the ESP_info parameter, together with the respective HITs and host identities

The problem with the mobilty exchange, when the host is behind a NAT, is that the address in the LOCATOR parameter is a private address and not globally routable.

[Editor's Note: Some possible solutions, to overcome this problem, are to use RVS server as a contact point, initiator should find the public address and somehow has to inform it to the responder and the NAT has to bind the new private address and the public address.]

In case of multihoming scenario, in which the hosts can be reached by several addresses, the NAT handling becomes complicated. For example, if a host is multihomed, assume that the initial HIP and security associations are established with a public IP address of the host. Later, if it decides to use the address which is behind a NAT, then the "new" NAT has to create a binding between the hosts.



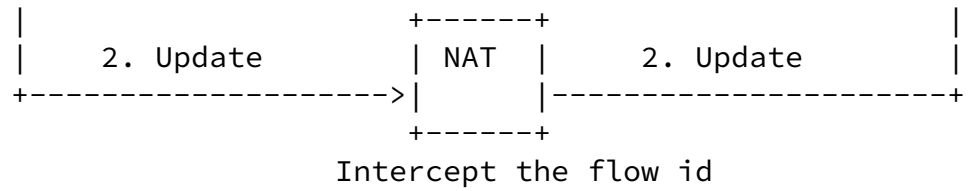


Figure 7: Multihoming and Middleboxes

Figure 7 depicts the one possible scenario in which the initiator is multihomed.

1. If the Initiator notices the change, it can update the new address by using "Locator" parameter in the UPDATE messages (or can inform the NAT). By this way, a NAT can create a new binding by intercepting the UPDATE messages.

2. If the Responder itself decides to send the traffic to the previously exchanged address (informed as alternative address), then the NAT will disrupt the connection, since it does not have necessary state information to handle the traffic. A more detailed analysis, about multihoming, will be done in the future version of this draft.

5. Scenarios

The following section describes some example scenarios, in the context of involving middleboxes, to learn the flow identifier:

5.1. Different Firewalls at Initiator for outgoing and incoming packets

This scenario assumes that both the initiator I and the responderR is situated behind firewalls named FW(I) and FW(R) respectively. FW(I) is for the incoming packets to I and FW(R) is for the incoming packets to R. It is necessary that both the firewalls must learn the

flow identifier information and should store the state <SPI,IP,HIT> to forward IPsec protected payload packets. This scenario is illustrated in Figure 8

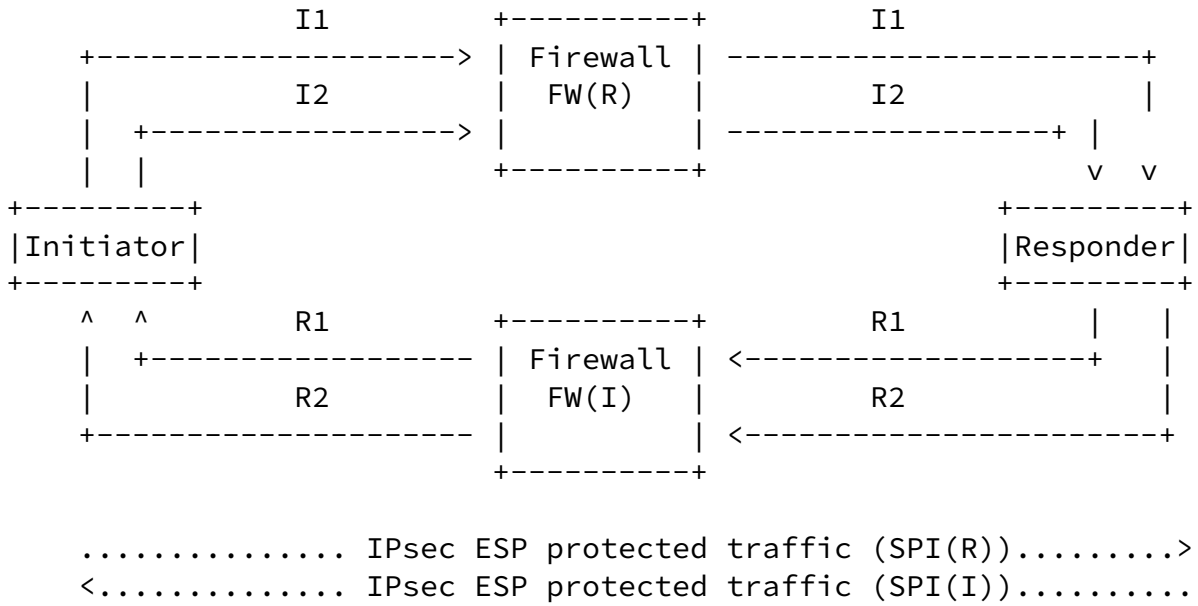


Figure 8: End hosts behind FWs

1. I1 packet is sent from the initiator I to responder R.

2. FW(R) forwards the packet to the Responder.

3. Then, R sends R1 message with puzzle,D-H key protected with the signature of R.

4. FW(I) forward the packet to the Initiator.

5. Now, I sends the I2 packet, on receiving I2, FW(R) verifies the signature of I and learns the SPI value form the ESP_info parameter and forwards it to the Responder

6. To complete the base exchange, R sends the message R2 to I.

7. On receiving R2, FW(I) verifies the signature of R. Accordingly, it earns the SPI value from the ESP_info parameter and forwards it to the Initiator.

Here, the problem with this asymmetric base exchange is that the SPI needed for the FW(I) is sent through the I2 message, which flows through the FW(R) and the SPI needed for for the FW(I) is sent to FW(R).

The topology shown in Figure 8 shows a scenario where messages R1/R2 are traversed by middlebox FW(I) and messages I1/I2 traverse middlebox FW(R). These scenarios might be found in larger networks with routing asymmetry and multi-homed networks. Today, in many cases a state synchronization protocol is used between these two middleboxes to make them apear as a single device and therefore avoiding problems.

A solution for dealing with NAT traversal is simpler compared to firewall traversal. With one single NAT between the HIP nodes, all messages of the base exchange are forced to pass through it. With firewalls, it becomes obvious that the nice property of a NAT with respect to the symmetric forwarding path is lost and here the individual firewalls are unable to create the necessary firewall pinholes. SPI(I) is exchanged in I2 message (ESP_info(I)) through firewall 1, however firewall 2 only needs it. Similarly firewall 2 needs SPI (R) which is sent in message R2 (ESP_info(I)) through firewall 1.

Hence, problems related with routing asymmetry and firewall traversal are :

1. When hosts are behind multiple incoming firewalls, they are unable to decide to which firewall they have to signal the appropriate SPI values.

2. The second problem is to secure the SPI signalling message from the end host to the FW. Since the end hosts authenticate and authorize to the FW that lets outgoing packets, they share keys only with them. However, as mentioned earlier, they, somehow, need to signal the SPI value to the FW on the other end which forwards incoming packets.

5.2. Data Receiver behind a NAT

This scenario explains the full operation during the HIP base exchange between the Initiator and the Responder, where the Responder is assumed to be situated behind a NAT and registered with the rendevous server (RVS) to facilitate its reachability.

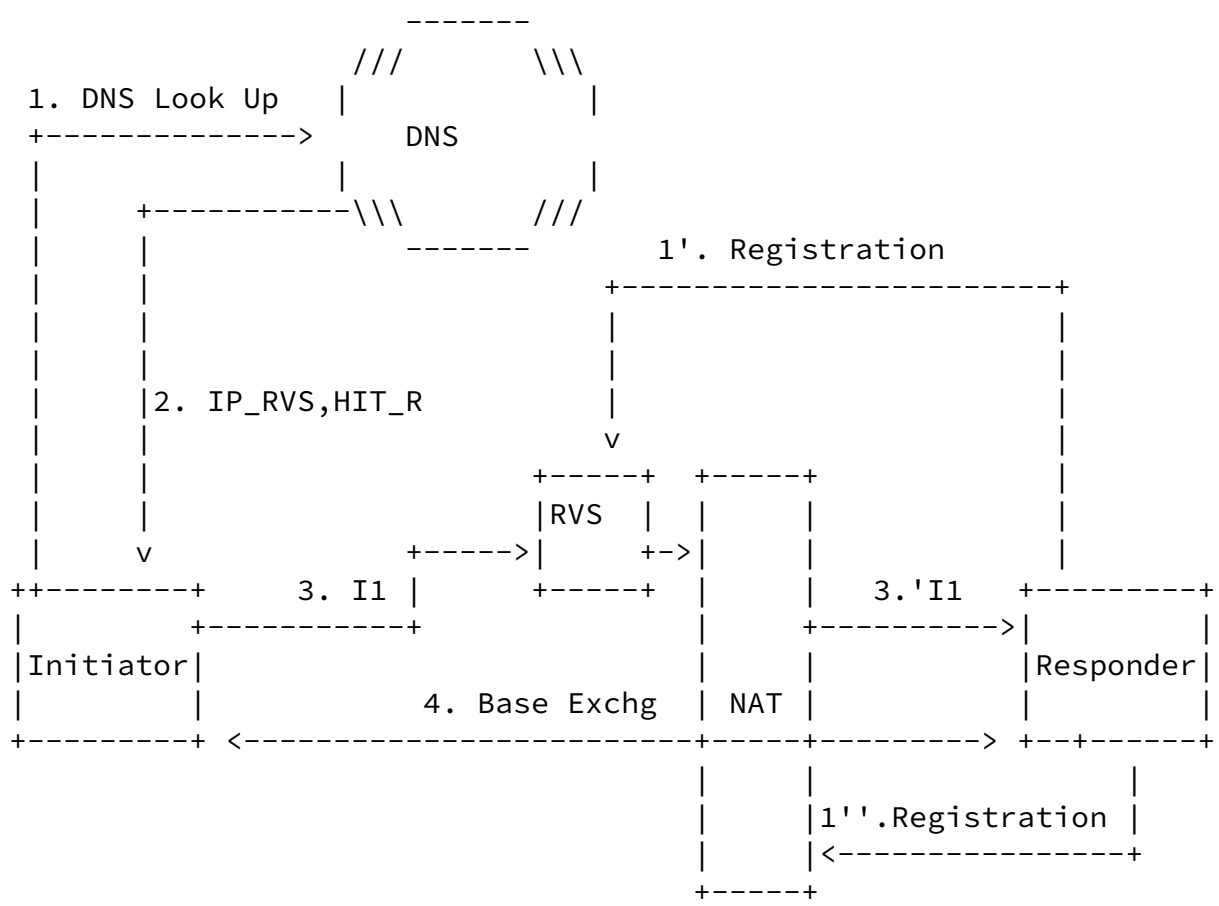


Figure 9: HIP Responder with RVS and NAT

Figure 9 shows the pictorial representaton of the operation.

- Initiator looks up the DNS in order to find the connection parameters for the responder, This is typically done by querying the DNS with the corresponding FQDN.

- Since the responder is registerd with the RVS, the DNS record will contain the IP of the RVS and the HIT of the responder.

- The Initiator, now, contacts the RVS by sending I1 message, the RVS relays the message to the responder. If the responder is situated behind a NAT, it must inform the NAT, beforehand, to

allow the HIP base exchange packets to be traversed via the NAT.

This typically requires a registration mechanism to siganl the NAT.

- The NAT forwards the HIP packets and actively participates in the base exchange. If ESP traffic information is exchanged, the middlebox will also learn the flow identifier.

Here, the NAT might require authentication and authorization from the endhosts in order to enable a NAT binding for the requesting hosts. This can be done achieved by performing middlebox signaling, the requirements for such solution is explained in Section 6.

6. Requirements for HIP Middlebox Solution

This section presents a few high-level requirements that are derived from the given problem statement. A novel middlebox signaling approach has to accomplish the following goals:

- Add some authentication and authorization capabilities to the NAT/Firewall traversal. Many NAT/Firewall traversal solutions do not allow the end host to interact with the middlebox. As a consequence, some security vulnerabilities are introduced e.g.,denial of service.

- Add secure firewall traversal functionality as another type of middlebox signaling by using <destination IP address, SPI and protocol> triplet. as a substitute for the traditional < source IP, destination IP, source port, destination port, transport protocol> information.

It is recommended that a solution for HIP-aware middlebox signaling needs to have the following properties:

- A HIP-aware NAT/FW MUST be able to authenticate the entity requesting a NAT binding or a firewall pinhole.

- A HIP-aware NAT/FW MUST be able to intercept HIP messages in order to extract the flow identifier information and other related information. A HIP-aware NAT/FW MUST be able to distinguish these messages.

- A HIP-aware NAT/FW MUST authorize the entity requesting a NAT binding or a firewall pinhole before storing state information. This requirement might be accomplished by identity based authorization or an identity independent authorization mechanism.

- o A NAT/FW node MUST NOT introduce denial of service attacks.

- o A potential solution MUST respect the property of some middleboxes which do not allow traffic (data and signaling traffic) to traverse the middlebox without proper authorization.

Some requirements are taken from [I-D.ietf-nsis-nslp-natfw].

7. Security Considerations

In this document, a problem statement is given and scenarios are described that lead to a number of requirements, which focusses on security at a higher level of abstraction. However, this document does not perform a detailed security analysis for a HIP-aware middlebox solution.

The authors recommend that, atmost care should be taken when solutions are developed and the solution must not introduce new security vulnerabilities to the middlebox.

8. Contributors

We would like to thank Aarthi Nagarajan, Vesa Torvinen, Jochen Grimminger and Jukka Ylitalo for their help with initial versions of this document.

9. Acknowledgements

The authors would like to thank Pekka Nikander, Dieter Gollmann and Tuomas Aura for their feedback to this document.

This document is a byproduct of the Ambient Networks Project, partially funded by the European Commission under its Sixth Framework Programme. It is provided "as is" and without any express or implied warranties, including, without limitation, the implied warranties of fitness for a particular purpose. The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or

endorsements, either expressed or implied, of the Ambient Networks Project or the European Commission.

10. References

10.1. Normative References

[I-D.ietf-hip-base]

Moskowitz, R., "Host Identity Protocol", draft-ietf-hip-base-06 (work in progress), June 2006.

[I-D.ietf-hip-esp]
Jokela, P., "Using ESP transport format with HIP", draft-ietf-hip-esp-04 (work in progress), October 2006.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", March 1997.

10.2. Informative References

[I-D.ietf-hip-mm]
Nikander, P., "End-Host Mobility and Multihoming with the Host Identity Protocol", draft-ietf-hip-mm-04 (work in progress), June 2006.

[I-D.ietf-nsis-nslp-natfw]
Stiemerling, M., "NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", draft-ietf-nsis-nslp-natfw-12 (work in progress), June 2006.

[I-D.irtf-hiprg-nat]
Stiemerling, M., "NAT and Firewall Traversal Issues of Host Identity Protocol (HIP) Communication", draft-irtf-hiprg-nat-03 (work in progress), June 2006.

[I-D.nikander-hip-path]
Nikander, P., "Preferred Alternatives for Tunnelling HIP (PATH)", draft-nikander-hip-path-01 (work in progress), March 2006.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, November 1998.

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3715] Aboba, B. and W. Dixon, "IPsec-Network Address Translation (NAT) Compatibility Requirements", RFC 3715, March 2004.

[RFC3947] Kivinen, T., A. Huttunen, A., Swander, B., and V. Volpe, "Negotiation of NAT-Traversal in the IKE", RFC 3947, January 2005.

[RFC3948] A. Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec Packets", RFC 3948, January 2005.

[RFC4080] Hancock, R., "Next Steps in Signaling: Framework", RFC 4080, November 2004.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC RFC4303, December 2005.

[RFC4306] Kaufman, C., "Internet Key Exchange (IKEv2) Protocol", RFC 3948, September 2004.

[RFC4423] Moskowitz, R. and P. Nikandar, "Host Identity Protocol (HIP) Architecture", RFC RFC4423, May 2006.

Authors' Addresses

Hannes Tschofenig
Siemens Networks GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bavaria 81739
Germany

Phone: +49 89 636 40390
Email: Hannes.Tschofenig@siemens.com
URI: http://www.tschofenig.com

Murugaraj Shanmugam
Siemens Networks GmbH & Co KG
Otto-Hahn-Ring 6
Munich, Bayern 81739
Germany

Email: murugaraj.shanmugam@siemens.com

Full Copyright Statement

Intellectual Property

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).