NSIS Working Group
Internet-Draft
Expires: August 16, 2004

C. Aoun
Nortel Networks
M. Brunner
M. Stiemerling
M. Martin
NEC
H. Tschofenig
Siemens

February 16, 2004

NAT/Firewall NSLP Migration Considerations
draft-aoun-nsis-nslp-natfw-migration-01

Status of this Memo

Copyright Notice

Abstract

This document discusses migration issues towards NSIS NAT/FW NSLP enabled NATs and Firewalls. The document will serve as input to the NSIS NATFW NSLP document.

Table of Contents

1. Introduction

The overall NSIS protocol suite (including the NATFW NSLP) is impacted by NSIS NATFW NSLP unaware NATs and Firewalls, this document covers impacts as well as some suggestions to ease the deployments of the NSIS protocol suite until the installed base on NATs and Firewalls migrates to NSIS.

The NATFW NSLP should allow an end host supporting NSIS to operate properly without the need of supporting true end-to-end NSIS signaling to its application correspondent. This is very practical during the initial phases of the NSIS migration and is applicable in simple network configurations not affected by asymmetric routing. In the early phases of the NSIS NATFW NSLP migration, this situation will occur quite frequent and hence this scenario must be supported.

The NSIS protocol should traverse NSIS unaware NATs (and possibly Firewalls) to allow a smoother deployment of, for example, Qos NSLP in today's networks. To provide a smooth migration it is necessary to understand the coexistence of NSIS aware and unware NATs and Firewalls.

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 [1].

The terminology used in this document is defined in [2].

3. NSIS unaware NAT Traversal

This section discusses how an NE with any NSLP could still operate when an NSIS unaware NAT is on the data path. The detection of an NSIS unaware NAT could be a feature of the NTLP [3], allowing its usage on any NE regardless of the supported NSLPs.

Several NSIS independent approaches could be used by the NE to learn its global scoped address in order to use it for its hosted NSLPs. In this version of the document, only the STUN protocol [5] is considered as means to acquire the global scoped address; the next versions will consider other approaches.

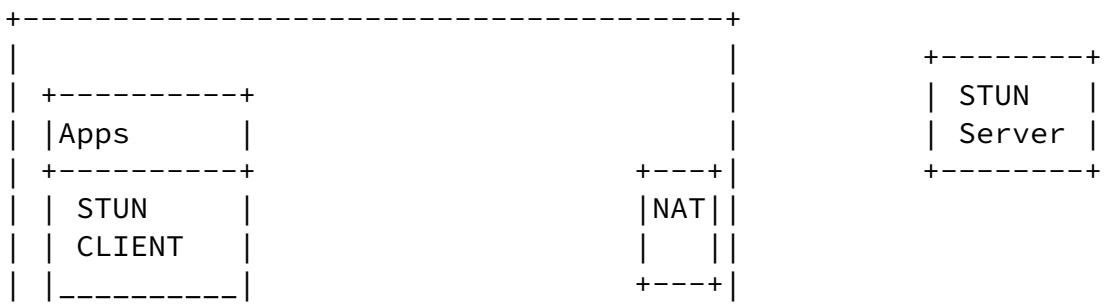
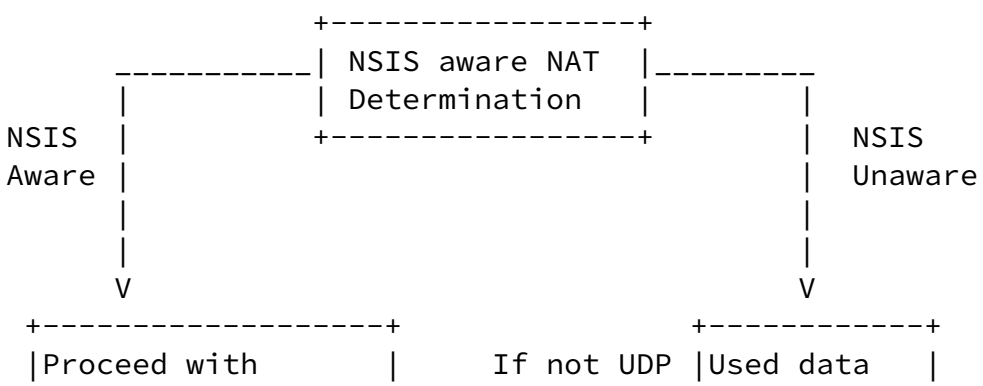
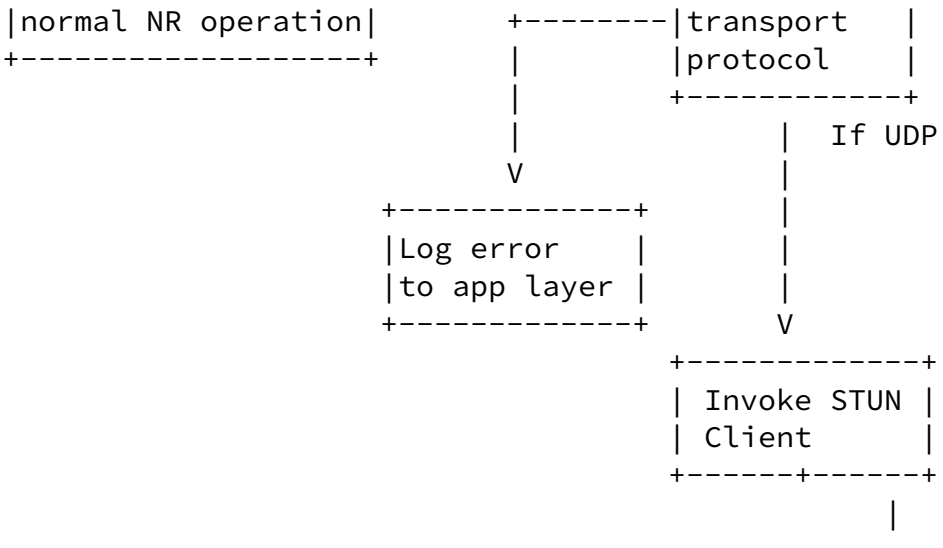


Figure 1: STUN usage for NSIS unaware NATs

Within the initial stages of the NSIS migration, NE functions will be co-hosting a STUN client that was already present on the application end-host. Within Host A, shown in Figure 1, the NSIS API could invoke the services of the STUN client (as shown in Figure 2) upon determination that an NSIS unaware NAT was on the path.This would allow applications using UDP transport to work (only applicable for cone NAT variants [5]).





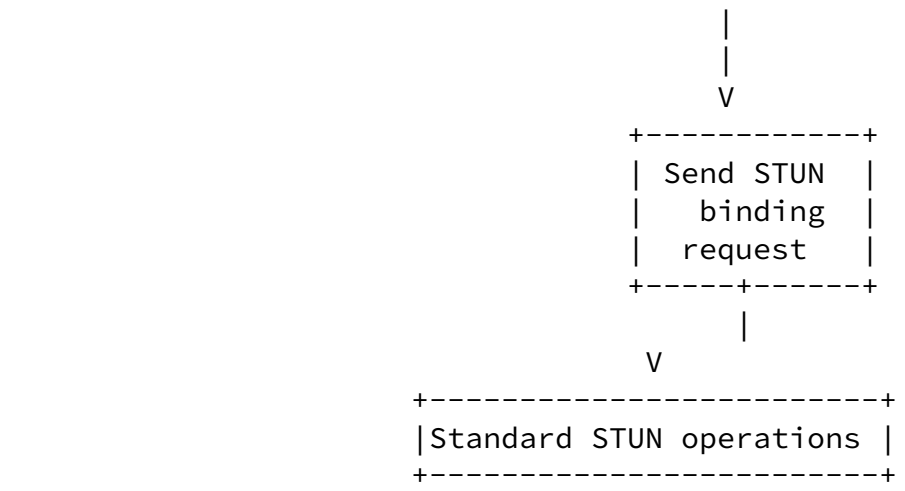
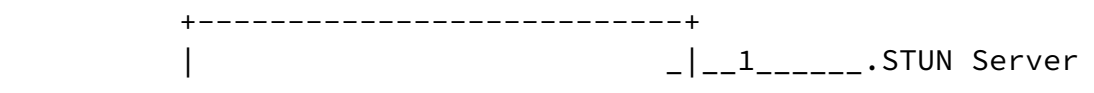


Figure 2: Interactions with a STUN client

NSLPs would use the STUN returned global scoped address for the flow id [3].To allow NSIS signaling to be received by the NR on host A, without impacting existing applications (i.e. without explicitly providing the address and port of the NSIS recipient in the application signaling), the NSIS protocols would need to use NTLP datagram mode transport (as defined in [3]). This would imply that the NTLP will be using the same port as the data flows, this might complicate the proposed mode of operations (and might not meet the expected performance). The next version of the draft will discuss whether this approach would be practical based on received feedback from implementors.

Subsequently we discuss how the NATFW NSLP could co-exist with interim NAT traversal mechanisms described in [8]. In Figure 3, a STUN client (Host A) [5], an NE (Host B), a host using a Media Proxy [8] and host using a TURN client [9] co-exist in the same network with a NATFW NSLP aware NAT. There are no reasons for the existing mechanisms to be mutually exclusive every host could continue using

the existing interim solutions, meanwhile the unilateral NSIS signaling would be used until both ends support the NSIS NATFW NSLP.



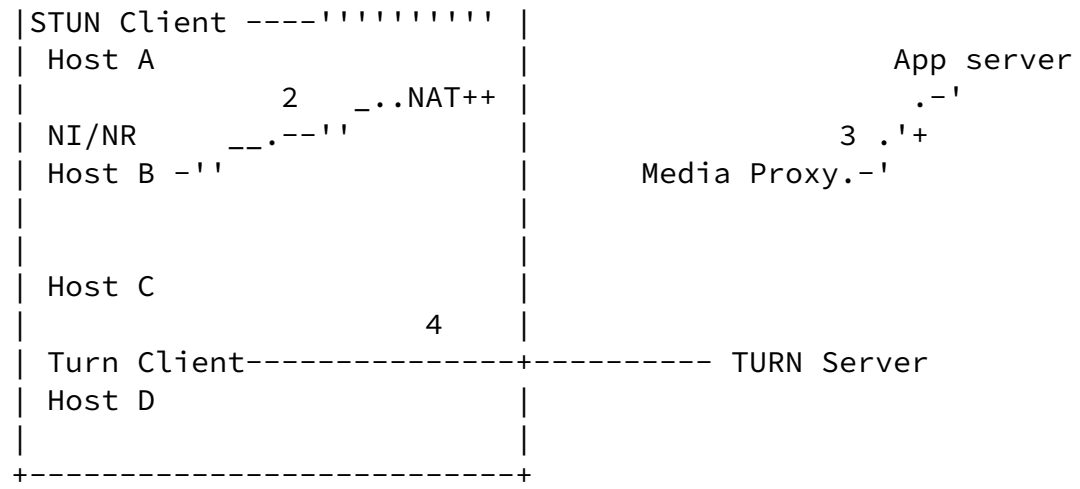


Figure 3: Coexistence of NSIS NATFW NSLP and existing NAT traversal mechanisms

4. Unilateral NSIS signaling

When NSIS NAT/FW signaling will start to be deployed, it is quite possible that an NI sends an NSIS message without having an NR to respond to it. The NATFW NSLP should be able to handle this type of deployments. NSIS NATFW NSLP signaling for NAT binds is already local within the trust domain (the Reserve External Address is intercepted by the edge NAT, ref [2], however this is not the case with firewall signaling that should be end to end.

Since the purpose of this section is to discuss how are end to end signaled messages handled when no NRs are available on the end-host only Firewalls (the NFs) are discussed within the example networks.

There are two interesting cases to be analyzed:

Approach 1: Implicit (not explicitly scoped) localized signaling: The local trust domain (from an NI perspective) has at least one NSIS aware Firewall, there is no NR on the far end as well as no NSIS aware NAT or Firewall. This approaches is similar to [13], however the NSIS messages do not included any scoping information. Figure 4 shows this scenario graphically.

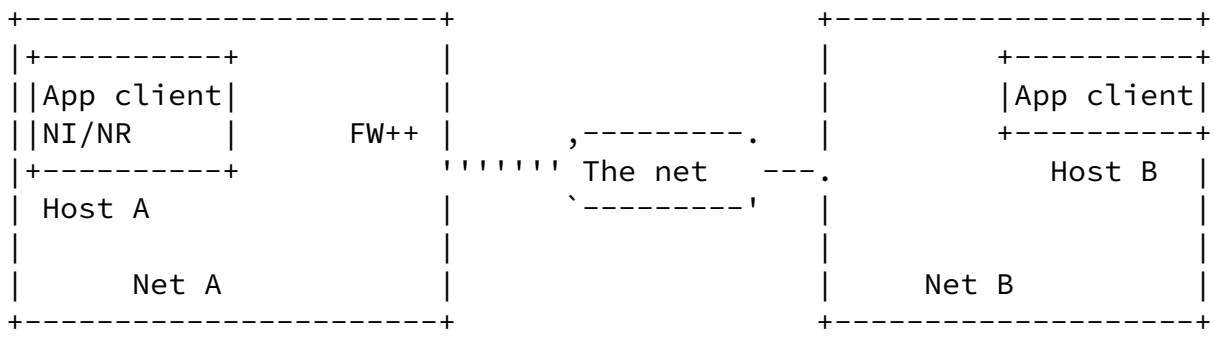


Figure 4: Implicit localized signaling

Approach 2: Missing trust with far end host's NFs: The local trust domain has no NSIS aware Firewall, there is no NR at the far end but there is at least an NSIS aware firewall with which the local NI has no direct trust relation (which implies an authorization issue and possibly authentication issues). The main addition to the issue discussed in the localized signaling case above (determination of the last NE on the path and response to the NSIS message by the last NE) is the lack of trust relations with the NI. Figure 5 shows this scenario graphically.

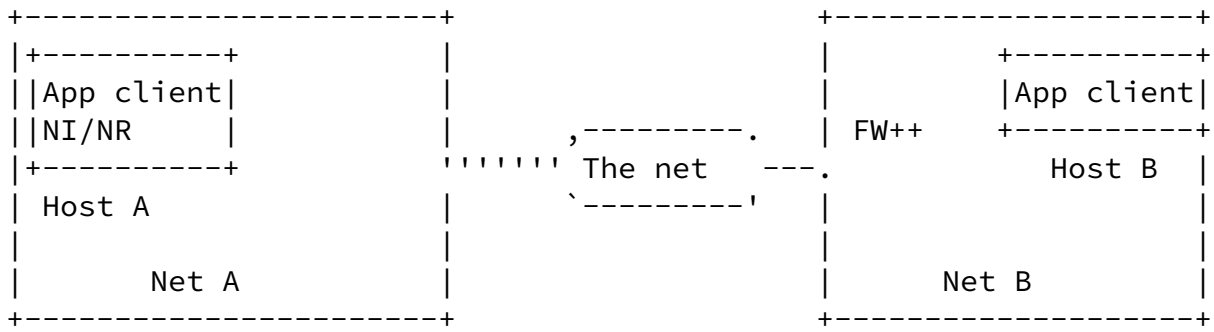


Figure 5: Missing trust with the remote host's network

In approach (1), the NI sends its firewall policy rule creation message, it traverses the first NF (its own firewall) but there is no NR to respond back. If we consider to have a response timer on the last NF being traversed by an NATFW NSLP message then if no response is received to the NSIS message, the last NF will respond back to the NI with a notification of no far end NR response. This will imply that the signaling will be scoped to the last NF on the path that responded back. Using the network deployment shown in Figure 4, the following mode of operation would apply:

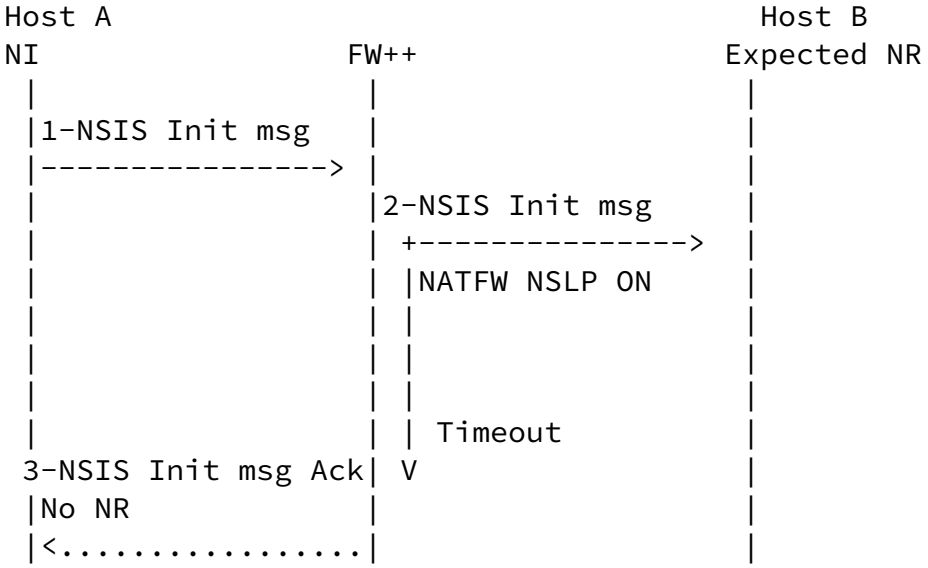


Figure 6: Detecting the last NSIS peer

Figure 7 provides the message sequences when more than one NSIS aware

NAT or Firewall is deployed within the same trust domain. Upon determination of a previous NSIS hop, an NSIS aware node will notify the previous NSIS hop of its existence to avoid launching the timer that triggers sending of an NSIS message back to the NI. The current NTLP message association establishment procedures supports this

behavior. The last NF on the path will launch the timer since no valid downstream NSIS neighbor responded back.

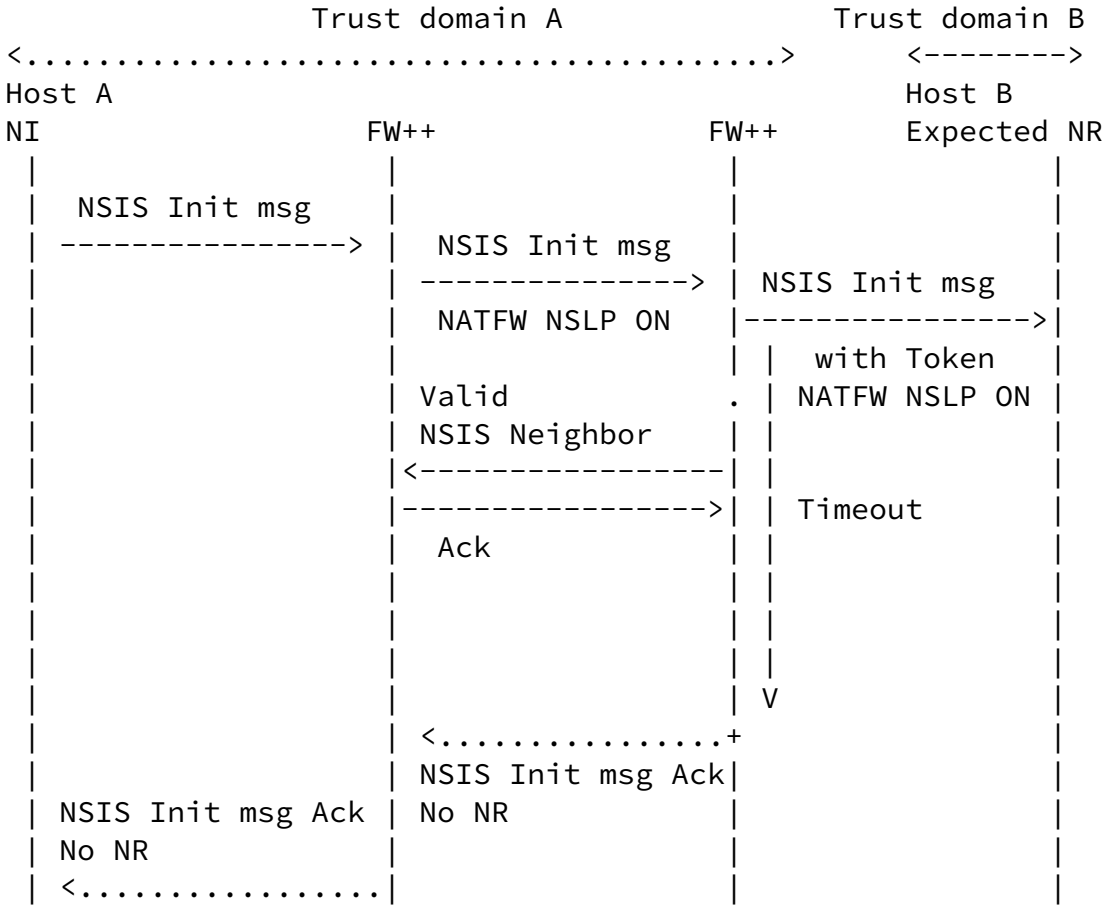


Figure 7: Detecting the last NSIS peer (multiple FWs)

In approach (2), the NI sends its firewall policy rule creation message, it traverses the FW hosted in Host B's network, but host A is not authorized to install a policy rule unless the policy rule creation is approved by a trusted entity within Net B. Unfortunately Host B was not yet upgraded to support the NATFW NSLP, another entity

needs to authorize the policy rule installation.
Potentially a trusted third party already aware of the application session held between Host A and Host B could provide an authorization token to Host A [11], the token would be encapsulated within the NATFW NSLP message and would allow the NSIS aware Firewall in Net B to authorize Host A's requested policy rule to be installed. This approach would obviously require to put in place a mechanism to provide the authorization token to Host A. The token could be requested by the NI and included in the NSLP signaling by default or after receiving an error message from the far end NSIS aware Firewall indicating that authorization data is required. The authorization token would need to be associated with the identity of the NI,

associating the authorization token with an IP address is not sufficient, and could lead to issues if the IP address was not valid due to address translation occurring on the path, a proper mechanism should be put in place to allow proper authentication of the entitled token user.

Figure 8 shows the architecture with two different networks and the trusted third party which creates the authorization. Figure 9 provides a message flow for authorization token handling.

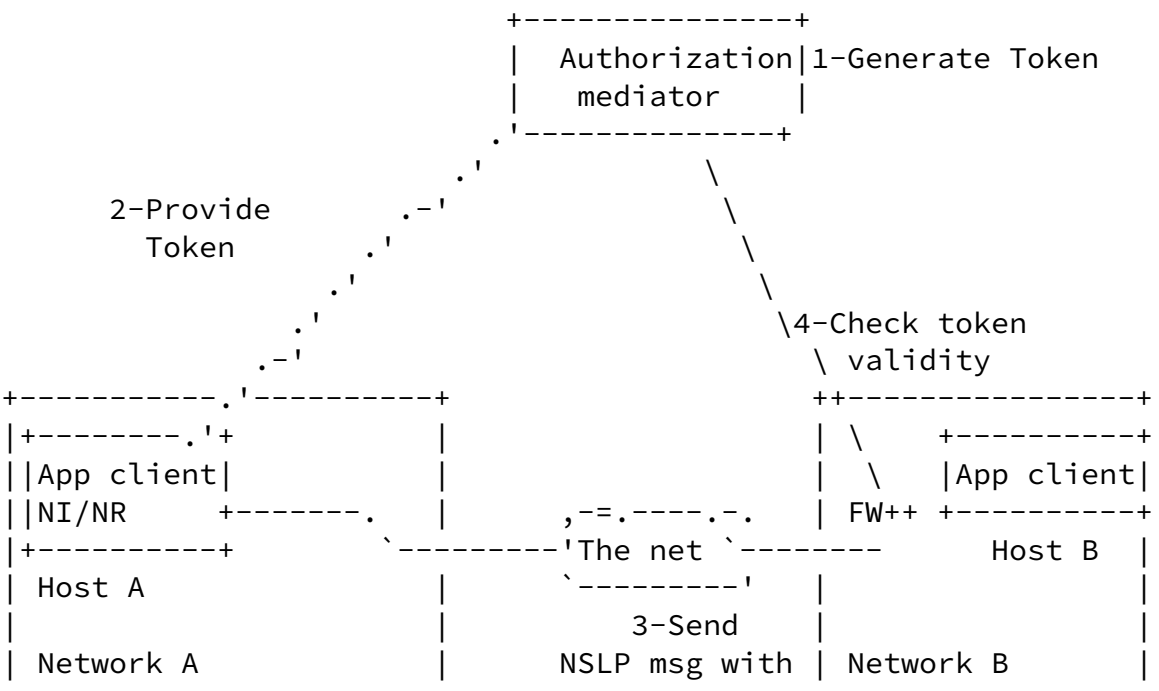
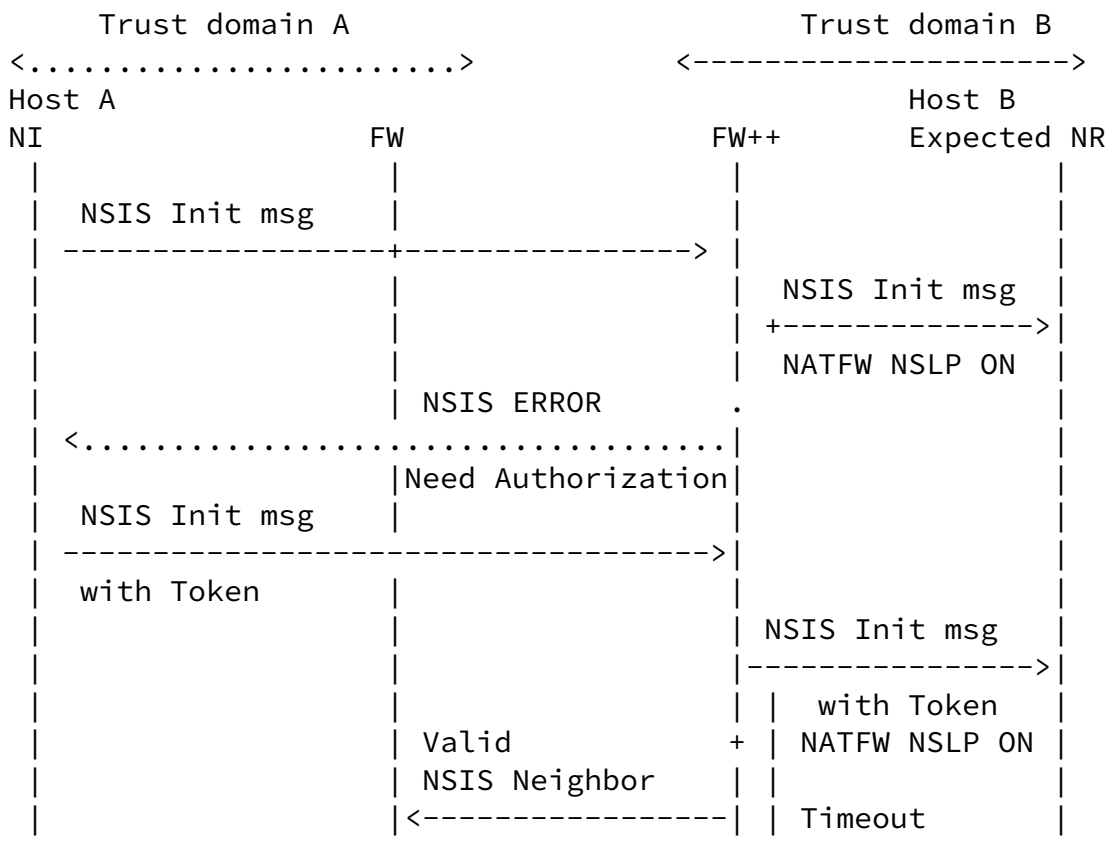


Figure 8: Authorization Token Handling



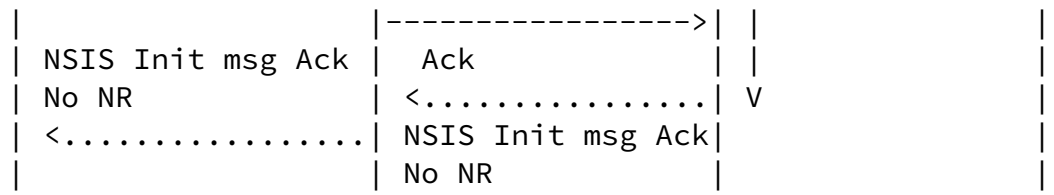


Figure 9: Authorization Token Message Flow

5. NSIS unaware Firewall Traversal

In case an NSIS unaware firewall is traversed by NSIS messages, NSIS messages should be allowed to go through it, as well as the exchanged data flows between the user application clients. This is not necessarily an obvious task to perform in case the NSIS messages cannot be identified by the NSIS unaware firewall. Same applies for the user application data flows.

NSIS message identification should be supported by existing firewalls.
Currently firewalls support flow identification by using the 5 tuple or a sub-set of it. The authors are still expecting feedback from firewall vendors to see if we can assume that existing firewalls will not drop packets including the the Router Alert Option (RAO) [12]. In

case existing firewalls drop packets having the router alert option, then the RAO should not be the only element of the used identification filter.

User application data flow identification, should be deterministic at a specific address and port range level. This means that the application clients uses a combination of an address and specific transport port range.This combination should be configured on the firewall.

In case a NAT is deployed on the path and it is NSIS-NATFW, the assigned bind should be consistent with policy rules configured with the NSIS unaware firewall.

Even though the deployed Firewall is not NSIS aware, the application data would still be forwarded if existing interim solutions were used such as a mix of stateless policy rules and flow based states with initial packets sent in the outbound direction (inside to outside a trust domain).

6. NATFW NSLP NTLP requirements

In this section we list two requirements for the NTLP raised by this document.

- When NSIS signaling is used in presence of NSIS unware NATs then raw IP MUST NOT be used. Network address and port translation requires transport layer identifiers as mean to direct inbound

traffic to the right recipient.

- If IPsec is used to secure NSIS signaling messages then UDP encapsulation for IPsec protected packets (see [4]) MUST be used to ensure that IPsec does not break. IKE with extensions or IKEv2 is able to detect the presence of a NAT along the path.

7. Security Considerations

This document discusses various security issues for NAT/Firewall signaling in migration scenarios.

Further security considerations can be found in [2].

8. Open issues

Working on this document we identified to the following open issues and actions that need to be taken:

- Add a network centric solution to address interim deployment phases where the end host doesn't support yet the NSIS protocol suite.
- Provide updates on the RAO firewall issues
- Update Section 3 with regards to the multiplexing/demultiplexing of NSIS messages and user data on the same socket.
- Move the mediated authorization discussion in Section 4 to [2]

Normative References

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

[2] Stiemerling, M., Martin, M., Tschofenig, H. and C. Aoun, "A NAT/Firewall NSIS Signaling Layer Protocol (NSLP)", DRAFT draft-ietf-nsis-nslp-natfw-01.txt, February 2004.

[3] "GIMPS: General Internet Messaging Protocol for Signaling", draft-draft-ietf-nsis-ntlp-00 (work in progress), October 2003.

Informative References

[4] A. Huttunen et all, A., "UDP Encapsulation of IPsec Packets", DRAFT draft-ietf-ipsec-udp-encaps-07.txt, Jan 2003.

[5] Rosenberg, J., Weinberger, J., Huitema, C. and R. Mahy, "STUN - Simple Traversal of User Datagram Protocol (UDP) Through Network Address Translators (NATs)", RFC 3489, March 2003.

[6] Handley, M. and V. Jacobson, "SDP: Session Description Protocol", RFC 2327, April 1998.

[7] ITU-T SG16, "Packet-based multimedia communications systems", ITU-T H.323, November 2000.

[8] Rosenberg, J., "NAT and Firewall Scenarios and Solutions for SIP", draft-rosenberg-sipping-nat-scenarios-00 (work in progress), November 2001.

[9] Rosenberg, J., "Traversal Using Relay NAT (TURN)", draft-rosenberg-midcom-turn-01 (work in progress), March 2003.

[10] Swale, R., Mart, P., Sijben, P., Brim, S. and M. Shore, "Middlebox Communications (midcom) Protocol Requirements", RFC 3304, August 2002.

[11] Hamer, L-N., Gage, B. and H. Shieh, "Framework for Session Set-up with Media Authorization", RFC 3521, April 2003.

[12] Katz, D., "IP Router Alert Option", RFC 2113, February 1997.

[13] Manner, J., "Localized RSVP", draft-manner-lrsvp-03 (work in

progress), January 2004.

Authors' Addresses

Cedric Aoun
Nortel Networks

France

EMail: cedric.aoun@nortelnetworks.com

Marcus Brunner
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 905 11 29
EMail: brunner@ccrle.nec.de
URI: http://www.brubers.org/marcus

Martin Stiemerling
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36
Heidelberg 69115
Germany

Phone: +49 (0) 6221 905 11 13
EMail: stiemerling@ccrle.nec.de
URI:

Miquel Martin
Network Laboratories, NEC Europe Ltd.
Kurfuersten-Anlage 36

Heidelberg 69115
Germany

Phone: +49 (0) 6221 905 11 16
EMail: miquel.martin@ccrle.nec.de
URI:

Hannes Tschofenig
Siemens AG
Otto-Hahn-Ring 6
Munich 81739
Germany

Phone:
EMail: Hannes.Tschofenig@siemens.com
URI:

Intellectual Property Statement

rights which may cover technology that may be required to practice this standard. Please address the information to the IETF Executive Director.

Full Copyright Statement

Acknowledgment

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