NATFirewall NSLP Intra-realm considerations
draft-aoun-nsis-nslp-natfw-intrarealm-00

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

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 August 9, 2004.

Copyright Notice

Copyright (C) The Internet Society (2004). All Rights Reserved.

Abstract

This document discusses NAT/FW NSLP intra-realm issues and solutions. The document will serve as input to the NSIS NATFW NSLP document.
Table of Contents

1. Introduction ................................................. 3
2. Terminology ................................................. 4
3. Problem statement ............................................. 5
4. Potential solutions to the problem ............................. 9
   4.1 Intra realm solution protocol operation impacts ........... 12
   4.2 Intra realm solution application protocols impacts .......... 13
5. Security Considerations ....................................... 14
6. IANA Considerations .......................................... 15
7. Open issues .................................................. 16
   Normative References .......................................... 17
   Informative References ......................................... 18
   Authors’ Addresses ............................................. 19
   Intellectual Property and Copyright Statements .................. 21
1. Introduction

The NSIS NATFW NSLP responder provides the NSIS NATFW NSLP Initiator with its address, in some cases the NSIS responder may have several addresses: a (or several) global scoped address and its locally scoped address(es). Which address does it provide to the NSIS initiator? This document will cover the NSIS Responder address selection as well as the impact on the applications and the NSIS protocol suite. The document will serve as input to the NSIS WG documents.
2. Terminology

The terminology used in this document is defined in [1]
3. Problem statement

An NSIS Element hosting an NSIS NATFW NSLP may have more than one address, its local scoped address(es) and global scoped address(es). A default address selection that prioritizes arbitrarily a global scoped address over a local scoped address may imply non-optimal routing for communications between NSIS elements hosted within the same addressing realm.

In Figure 1 the arbitrary selection of the global scoped address, works properly to receive NSIS signaling from Host B. However in deployment scenario shown in Figure 2, host A and host C end-up communicating through their local MB1 middlebox resulting in a non-optimal data path with all its implications (additional delay, additional bandwidth in certain parts of the network infrastructure, etc ...).

Figure 1

+---------------------+                       +--------------------+
|                     |                       |                    |
| Host A              |     ,-----------.     |            Host B  |
|              +-----+|  ,-'The NET      '-.  |                    |
|              | MB1 |+--                   --+                    |
|              +-----+|  '-.             ,-'  |                    |
|                     |     '-----------'     |                    |
|                     |                       |                    |
+---------------------+                       +--------------------+

MB: Middle box (NAT or Firewall or a combination)
Host A: An NE hosting NSIS NATFW NSLP NI/NR capabilities
Host B: An NE hosting NSIS NATFW NSLP NI/NR capabilities
Figure 2

Figure 3 and Figure 4, show clearly the impact when the global scoped address is used to signal an NE within the same addressing realm. Figure 3 show how host A will use the Reserve External Address (defined in [1]) to get its global scoped address (i.e. the external address), same happens to host B. Figure 4 shows how the CREATE/CREATE ACK message (defined in [1]) are exchanged to host B/A global addresses and the impact on the data path.

MB: Middle box (NAT or Firewall or a combination)
Host A: An NE hosting NSIS NATFW NSLP NI/NR capabilities
Host B: An NE hosting NSIS NATFW NSLP NI/NR capabilities
Host C: An NE hosting NSIS NATFW NSLP NI/NR capabilities
--- NATFW NSLP signaling

=== User Application signaling (SIP, H323, MGCP, MEGACO etc)

Figure 3
Host C         Host A          MB1            App server/proxy
10.1.2.3       10.1.2.2       a.b.c.e          a.b.c.e

<table>
<thead>
<tr>
<th>CREATE</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>CREATE</td>
<td></td>
</tr>
<tr>
<td>CREATE ACK</td>
<td></td>
</tr>
<tr>
<td>CREATE ACK</td>
<td></td>
</tr>
</tbody>
</table>

App signaling continues ...

++++++

++++++

<table>
<thead>
<tr>
<th>App data</th>
</tr>
</thead>
<tbody>
<tr>
<td>++</td>
</tr>
</tbody>
</table>

--- NATFW NSLP signaling

--- User Application signaling (SIP, H323, MGCP, MEGACO etc)

Figure 4
4. Potential solutions to the problem

There are two ways to deal with this non-optimal routing of packets for intra-realm communications between NSIS entities. The NSIS Responder should either:

1. Decide based on local decision, which address to provide to the NI to signal it or,

2. Let the far end NSIS Initiator decide which address to select based on the NSIS Responder’s provided addresses

(1) lets the NSIS Responder decide on its own, which address to provide based on certain hints, which may not be the most optimal decision since the NSIS Responder may not have sufficient knowledge about the NSIS Initiator at the time of delivering its address via user applications. In most cases local decision for address selection requires to know about the far end host, which is not always practical.

An example of such local based address selection is the IPv6 default address selection mechanism ([2]) where an IPv6 (or IPv6/v4) node has to select which source and destination address to pick in order to communicate with a far end node. The mechanism relies on receiving input from the local resolver (DNS client or local hosts file) about the far end node. In the context of multimedia applications (and probably others as well), this address selection mechanism will not be sufficient since the far end application device is not necessarily known (the resolver client may return the address(es) of the application signaling and not the addresses of the actual application data flow recipient). Hence it can not decide successfully in all cases which address to provide to the NSIS Initiator.

(2) is more efficient as it requires the NSIS Responder to provide all its addresses (local scoped and global scoped ones) to the NSIS Initiator. The NSIS Initiator will need to decide on which address to signal the NSIS Responder among all the provided ones. One possible way for the NSIS Initiator to decide from which NSIS Responder address to use is to check on which address the NSIS responder will reply back. An existing proposal [3] discusses the usage of (2) for SIP User Agents (SIP UA), the SIP UA will probe the far end SIP UA to see from which address it will response back. In [3], the STUN protocol [7] is used to check the responsiveness of the far end host. In [6] the reverse routability, provided by the STUN response, is used to check which address to respond to counters RTP DOS attacks. The same reverse routability could be achieved by the NSIS NATFW NSLP.
In the context of NSIS, the NSIS protocol itself should be used as the probing mechanism. Consequently the NSIS Initiator will send simultaneously several NSIS messages towards the NSIS Responder, one message per provided address. Figure 5 and Figure 6 provide a good view of method (2).

In Figure 5 Host A (same one as in Figure 2) a Reserve External Address (REA) message which is intercepted by the edge NAT (in this case MB1). The edge NAT responds with a REA ACK message providing the External Address (the global scoped address) to host A. Once host A has collected all the addresses where it could receive application data it informs its Application server about the remote application...
party as well as host A’s data recipients addresses (and ports), 10.1.2.2 and a.b.c.e. The same will happen with Host C, and Host C will be able to respond with the application protocol to Host A about its data recipient addresses (local and global scoped ones). Figure 6 shows how the CREATE messages are simultaneously sent by A to all the returned addresses for C. Host A receives both CREATE ACKs, the local scoped address will therefore be considered as the address to use to send NSIS NATFW messages to C. Since no NSIS aware NAT and Firewalls are on the path between host A and host C (when using local scoped addresses), host A would either send a DELETE message or let the NSIS state expire on its own.

Host C         Host A            MB1          App server/proxy
10.1.2.3       10.1.2.2          a.b.c.e            a.b.c.e
|              |    CREATE 2    |                  |
|   CREATE 1   | -------------> |--,               |
| <------------|                |  |               |
| CREATE ACK 1|                |  |               |
| ------------>|    CREATE 2    |  |               |
| <--------------------------|<-'               |
| CREATE ACK 2|                |  |               |
| ------------->|--,               |
|                | CREATE ACK 2 |  |               |
| <---------------|<-',               |
| App signaling  continues ...             |
| <================================================================>
| <================================================================>
| ++++++++++++++++++               |
| App data               |
| <++++++++++++++++++          |
| exchanges               |

---- NATFW NSLP signaling

==== User Application signaling (SIP, H323, MGCP, MEGACO etc)

Figure 6

The following occur during the process:
In case the NSIS Responder and Initiator are located within the same addressing realm, the NSIS Responder should receive a response from all the addresses to which it has sent NSIS messages. The NSIS Initiator will then choose the local scoped address as the destination address for messages destined to the NSIS Responder.

In case the NSIS Responder and Initiator are not located within the same addressing realm, the NSIS Initiator would only receive a response from the valid global scope address. In event that there is another NE within the network that has the same local scoped address as the originally targeted NSIS Responder, the wrongly targeted NSIS Responder should send back an error or discard the message (the later would be preferable).

4.1 Intra realm solution protocol operation impacts

As opposed to the normal NSIS mode of operation, an NI that has already a security association with the neighboring NE on the path to a specific NR would need to verify that the target local scoped NR address is the same as the one already cached in its NSIS neighbor table cache (association of Next hop NE with the target NR table). This would be required to avoid any confusion with an NSIS node that could be hosted within the same addressing realm and that would have the same local scoped address.

There is a potential threat where a malicious NE with the same local scoped address as the target NR respond back positively to the NSIS message and consequently hijack the data flow. This threat could be counter-measured by requiring the NR to respond back with a challenge response information communicated by the application signaling (assuming that the application was secured).

The procedure requiring an NSIS Initiator to send NSIS messages to several NR addresses, requires that the NI sends his NSIS messages at the same time to avoid impacting real-time sensitive applications. In case the response to the message sent to the global scoped is received first, it could potentially be used as a hint that no response will be received from the NR’s local scoped address. Hence there is no point to continue to delay the address selection process and proceed with the NSIS protocol operations. This assumption may not be always applicable depending on the network topology and network load at the moment of the protocol message exchanges. In case the first response is received from a local scoped address and has successfully provided the challenge response material provided by the application signaling protocol then the address selection process ends, and the NSIS protocol operations continue.
4.2 Intra realm solution application protocols impacts

The proposed intra realm path optimization proposal requiring an NR to provide several data recipient addresses within the application protocol, has obviously a certain impact on the application protocol. [5] discusses the impact to SDP [8] and should be used by all the application protocols using SDP. A similar approach should be followed by other protocols, not using SDP, including H.323 [9] and others requiring usage of NSIS with multiple addresses for the NR. In addition the application signaling needs to provide a challenge response allowing the NR to respond back properly. This information either need to be added to the application protocols or existing protocol fields need to be used (preferred way).
5. Security Considerations

The challenge response approach helps in checking if the responding NR is the correct one, however the method has an issue in case the responding NR is not the end application host (this would be the case when the application end host does not yet support the NATFW NSLP). External means to the NSIS protocol suite need to ensure that the last NSIS hop responding on behalf on the application endpoint provide the challenge response information.
6. IANA Considerations

There are no IANA considerations defined in this document.
7. Open issues

- Get agreement on solving the problem and its associated security issue, is the challenge response sufficient?

- Get feedback on which parameter is used within certain application protocols (SIP, MEGACO, MGCP, H323) as the response parameter
Normative References

Informative References


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:
Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any intellectual property 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; neither does it represent that it has made any effort to identify any such rights. Information on the IETF’s procedures with respect to rights in standards-track and standards-related documentation can be found in BCP-11. Copies of claims of rights made available for publication 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 implementors or users of this specification can be obtained from the IETF Secretariat.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary 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

Copyright (C) The Internet Society (2004). All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to the Internet Society or other Internet organizations, except as needed for the purpose of developing Internet standards in which case the procedures for copyrights defined in the Internet Standards process must be followed, or as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by the Internet Society or its successors or assignees.

This document and the information contained herein is provided on an "AS IS" basis and THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIMS 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.

Acknowledgment

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