MIDCOM Working Group
Internet Draft
Category: Informational
Expires on February 2001

C.Aoun
S.Sen
Nortel Networks

August 2001

Required Information in Midcom Agents

<draft-aoun-midcom-agent-information-00.txt>

Status of this Memo

Abstract

This draft is part of a gladiator contest within the MIDCOM WG to determine what network topology information is needed at the Midcom agent.

By taking out application awareness from Middle Boxes in the networks, and keeping this application knowledge in the application devices (the Midcom Agents); sufficient information needs to be put in the Midcom Agent to allow them to fulfill their responsibility.

Table of Contents

Abstract...1
1 Introduction...2
2 Conventions used in this document................................2
3 Used Terminology in the draft....................................2
4 Middle Box examples and Midcom requirements......................2

4.1 Middle Boxes connected to two address realms...................3

4.2 Middle Boxes connected networks having overlapped addresses....5
4.3 Multi-homed Middleboxes acting as media proxies...............6
5 Summary...6
6 References..6
7 Acknowledgments...7
8 Author's Address..7
9 Intellectual Property Statement.................................7
10 Full Copyright Statement.......................................8

1 Introduction

The Midcom Agent (MA) should have sufficient information to request the Middle Box to open pinholes or perform NAT binds or other specific actions on packet flows.

This draft presents several types of Middle Boxes that could be deployed in networks and the type of information that a MA needs to have to perform it's tasks properly.

2 Conventions used in this document

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 RFC-2119.

3 Used Terminology in the draft

If : an interface, it could be logical (ATM VC, FR DLCI, PPP variants, IPSEC tunnel...) or physical.

Overlapped address networks: Networks having overlapping addresses

Loopback address: Address that is not linked to an interface

4 Middle Box examples and Midcom requirements

This section describes several Middle Boxes (MB) that are deployed in networks:
- Middle Box connected to two address realms (that don't have overlapped addresses).
- Middle Box connected to networks having overlapped addresses.
- Multi-homed Middle Box acting as a media proxy.

The first category include the residential and enterprise Middle

Boxes, the second includes the Provider Provisioned Middle Boxes or other Middle Boxes interfacing networks that have overlapped addresses and the third includes, for example, RTP Proxies that are commonly used to allow VoIP media to pass through a firewall which does not have application awareness nor supporting Midcom

4.1 Middle Boxes connected to two address realms

```
   ++++++++++++++++++++
   + Customer     If1 +
   + network  +++++---+       o o o o o o         +++++++++++++++++++
   +          +MB1+If2+-------o           o       +Telephony Service+
   +   If5----+++++   +      oThe Internet o------+ Provider        +
   + If4-----/   +    +       o o o o o o o       + ++++            +
   +       If3---+    +                           + +MA+            +
    ++++++++++++++++++                            + ++++            +
                                                  +++++++++++++++++++
```

This example covers Middle Boxes that can have two (or more) interfaces and connected to 2 address realms (the enterprise realm and the public realm).
The example MB has 5 interfaces. 3 of the interfaces (could be one in case of a 2 interfaces MB)are used to connect internal hosts (if3,4,5) and 2 interfaces (could just be one in case of 2 interface Middle Box)are used to connect to the customer's ISP (if1,2).

This MB is similar to all existing MB implementations, in that MB packet filtering profiles are bounded to interfaces.
In the case of the NAT function, the profile is unique to the MB.
For packet filters, 2 profiles may exist: one for the egress and one for ingress.

We shall not consider other networks (the model will still be unchanged) since the purpose of the draft is to determine what information the Midcom Agent requires to allow particular flows to traverse a Middle Box.

Primary things the Midcom Agent needs to know when it needs to ask a particular MB to apply certain tasks on a flow:
-Which MB the application flows will be traversing, this is currently out of scope of the MIDCOM WG
-How to address the MB (loopback address or another reachable address)
-Provide a matching or filter expression to enable the MB to identify the flow
-Which tasks or queries to execute (Open a pinhole, get a BIND ...)

What about the interface and the direction?
The direction information is relevant to the direction of the packets on the interfaces (coming in or going out of the interface).

When the MA will send the Midcom message, it will contain a flow matching expression and the action to apply to the flow. The MB will know which profile to update (i.e. which interface is traversed and which direction).
The direction is implied by the source and destination contained in the flow matching expression.

The routing software could determine based on the routing table, which interface the packets may traverse; the rule will then be added to the proper MB function profile.
If the packet might traverse several interfaces the rule will be set on all the related profiles.
There is a potential ambiguity when the source of the flow is not known.
Typically this is the case of VoIP applications where the receiver is known but not the sender (initially since not included in the SDP).
In this case, all packet filter profiles need to be appended with the new rule (including packet filters that are bounded to if3,4 &5).
Alternatively an optional parameter within the matching expression could be used to express the directionality of the flow.
As an example:
-WAN could mean that the flow is from devices external to the network (i.e. limiting the packet filter profiles to the ingress ones of If1 & If2)
-LAN could mean that the flow is from devices internal to the network (i.e. limiting the packet filter profiles to the ones of if3,4,5)

The usage of "LAN" could address certain enterprise networks where packet filters are introduced between certain departments (case where packet filter profiles on internal interfaces require to be updated with new rule set).

4.2 Middle Boxes connected networks having overlapped addresses

Provider provisioned middle boxes addresses subscribers that have outsourced their Middle Box services to their Internet Service Providers (ISP).

This example shows 2 customer networks that are provided:
  - The Internet connectivity service by the same ISP
  - Their telephony service by either the same or different
Telephony Service Provider (TSP)

```
   +++++++++++++              +++++++++++++
   +           +         If1  +ISP        +
   +Cust A     +--------------+--++++++   +
   + 10/8      +         If2  +  + MB1+   + If3   o  o  o o
   +++++++++++++          ----+--+    +---+----o            o
                         /    +  ++++++   +\
                        /     +++++++++++++ \  o Internet   o
                       /                If4 \-           o
                      /                         o o o o o
   ++++++++++        /                            +
   +        +       /                             +
   +Cust B  +-------                              +
   + 10/8   +                                +++++++++++++
   ++++++++++                                +TSP        +
                                             + ++++      +
                                             + +MA+      +
                                             + ++++      +
                                             +++++++++++++
```

The main difference between the previous example and this one is that the physical MB, is subdivided into several logical MBs. Each logical MB has it's own interfaces and MB function profiles.

The logical MBs need to be addressed with separate identifiers. This is separate from the loop address which was discussed previously.

To communicate with the logical MB, the MA will require to use the logical MB's identifier within the Midcom protocol.

There is potentially another variant in which even the logical Middle Box could be connected to "overlapped addresses" networks.

In this case, the Midcom Agent will need to inform the Middle Box about the address's realm (either source or destination)of the specified flow.

Both Middle Box identifier and the realm identifier should be optional parameters in the Midcom protocol.

Apart from the previous, the information required for the MA and provided to the MB via the Midcom protocol is similar to 3.1

4.3 Multi-homed Middleboxes acting as media proxies

```
   +++++++++++++              +++++++++++++
   +           +         If1  +ISP        +
   + A         +--------------+--++++++   +
   + private   +         If2  +  + MB1+   + If3   o  o  o o
   +++++++++++++          ----+--+    +---+----o            o
                         /    +  ++++++   +\
                        /     +++++++++++++ \  o Internet   o
                       /        /If5    If4  \-           o
                      /
                               /                o o o o o
   ++++++++++        /        /
   +   B    +       /    ++++++++++
   +private +-------     +   C    +
   ++++++++++            +private +
                         ++++++++++
```

This case can be considered a special case of the scenario depicted in Section 4.2. The MB1 in the above figure is a multi-homed RTP Proxy (which terminates an RTP session in one interface and initiates a new one from the other interface). Assume that networks A, B and C contain private IP addresses, which overlap. To allow a VoIP session through the Proxy, we need allocation of either two private IP addresses (if a call is made between networks A, B or C), or a private IP address and a public IP address (if a call is made between an endpoint in networks A/B/C and an endpoint in the public Internet). In this case the Agent needs to specify the interface (or realm) through which the media will traverse the MB in order to make the MB assign IP addresses and perform proper binding of the RTP media with the interface.

5 Summary

The main issue to resolve while deploying Midcom enabled Middle Boxes will be on providing the MB presence on the path of the flows to the MAs.

Manual configuration will be a BIG operational burden on the application service providers, and will not be the most common solution (ref [DSCVRYCA]).

Extending the syntax to allow the MA to address properly a MB

(logical or physical) or to provide a proper flow filtering expression is not a complicated issue.
The Middle Box discovery is still a key piece of the puzzle.

6 References

[MDCMFRWK]P.Srisuresh,J.Kuthan, J.Rosenberg," MIDCOM Architecture
& Framework",
Internet draft, draft-ietf-midcom-framework-03.txt

[MDCMREQ] R.Swale, P.Mart, P.Sijben, " Middlebox Control (MIDCOM)
Protocol Architecture and Requirements",
Internet draft, draft-ietf-midcom- requirements-02.txt
[DSCVRYCA] C.Aoun, " Network topology considerations in
the MIDCOM Architectural framework",
Internet draft, draft-aoun-midcom-network-00.txt

7 Acknowledgments

The author would like to thank the following people for their useful comments and suggestions related to this draft: Louis-Nicolas Hamer,

Julian Mitchell, Mick O'Doherty and others in Nortel Networks.

8 Author's Address

Cedric Aoun
Nortel Networks
33 Quai Paul Doumer
Paris La Defense
92415 Courbevoie Cedex
France
Email: cedric.aoun@nortelnetworks.com

Sanjoy Sen
Nortel Networks
2375 N. Glenville Drive, Building B,
Richardson, TX-75082
USA
E-mail: sanjoy@nortelnetworks.com

9 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.

10 Full Copyright Statement