Solving the Middlebox Problem

Juergen Quittek,
Martin Stiemerling, Marcus Brunner
Network Laboratories, NEC Europe Ltd.
Tel.: +49 6221 90511-15, Fax.: +49 6221 90511-55
Email: {quittek, stiemerling, brunner}@ccrle.nec.de
Middleboxes in IP Networks

• Definition (RFC3234)
  – “A middlebox is defined as any intermediate device performing functions other than the normal, standard functions of an IP router on the datagram path between a source host and a destination host.”

• Common Middleboxes
  – Firewall
  – Network Address Translator (NAT)

• Most middleboxes block more traffic than necessary and desired (conservative approach)

• Some key services do not operate over secure firewalls or over NATs
  – **IP telephony**, video conferencing, NetMeeting, …
The Middlebox Problem

- Middleboxes are essential network components
- Migration to IPv6 might reduce the number of NATs, but it will not remove firewalls
- Middleboxes are potential obstacles to (UDP) media streams
Approaches to Solving the Middlebox Problem

• **Goal:** Smart firewall function / smart NAT
  – blocking unwanted traffic in general
  – particularly allowing traffic related to specific services

• **Technical problem:** how to tell the middlebox?

• **Three approaches:**
  – “call agent”
  – path-coupled signaling
  – smart middlebox
Three Approaches to Middlebox Control

1. “Call Agent”
2. Path-coupled Signaling
3. Smart Middlebox
**Call Agent:**

**General Status**

- Well understood: “telco style” gateway controller
- **Problems**
  - topology-awareness required
  - call agents needed per domain
- **Solution components:**
  - e.g. SIP server extension
    - 3GPP IMS (IP MM Subsytem)
  - Signaling protocol
    - IETF MIDCOM
- To be completed rather soon
Usage Example

- IP phone call across NAT
- SIP server controls NAT
- Need of external IP address and port before secure NAT session can be established
Status of IETF MIDCOM WG

- Architecture & requirements done (RFC 3303/3304)
- WG chartered to select an existing protocol rather than develop one
- Semantics document
  - Extracted from rejected dedicated protocol
- Protocol Evaluation in 2002
  => SNMP was selected as 'base protocol'
- MIDCOM people are not happy, because
  - they don't really know SNMP
  - they dream of a small and simple specific solution
- SNMP people are not convinced, this is a good idea
  - SNMP was not really designed for this purpose
  - requirements were written with a transaction-oriented protocol in mind
Political Problems of MIDCOM Working Group

- **Protocol Complexity**
  - Initially, Guys from telco companies (Lucent, Marconi, Nortel, Alcatel, BT) wanted more complex functionality
  - IETF decided for simple protocol -> some guys left

- **Protocol Selection**
  - Majority of the WG members prefer a small, specific protocol
  - IESG blocked this

- **General Approach**
  - WG chair organized Bird of Feather session on path coupled signaling approach
  - Chair in favor of closing WG as soon as possible and starting work on path-coupled approach
  - IETF area director’s position
    - path coupled approach will be covered by Next Steps in Signaling (NSIS) WG
    - MIDCOM WG will be closed when MIDCOM MIB is complete

Next Steps in Signaling (NSIS) WG

- MIDCOM WG will be closed when MIDCOM MIB is complete

08.01.2004 9
Smart Middlebox: Status

- First very simple products available
  - SIP-aware SOHO firewall (Cisco)
- No middlebox signaling required!
- Problems:
  - firewall must interpret signaling
  - new signaling protocol requires middlebox modification
  - path coupled session signaling required
- Research work just started
Smart Middlebox Issues

- Policy based control per signaling protocol required
- New protocols are emerging
- Modular solution required
- Prototype: self-configuring modular firewall
  - firewall modules supporting individual protocols
    - SIP module allowing IP telephony across firewalls
    - RTSP module allowing video downstreaming
  - modules can be licensed and loaded individually
  - modules can be loaded dynamically
  - implemented as NetBSD loadable kernel modules

08.01.2004
Modular Firewall

IP Packet Filter Module

TCP Module

UDP Module

FTP Module

SIP Module

Kernel Space Modules

User Space Modules

Protocol De-multiplexer

Firewall Hook (IP/TCP/UDP)
Path-Coupled Signaling: Status

- Under investigation, “Internet style” solution
- Problems: authorization, authentication
- Solution components
  - path-coupled signaling protocol (IETF NSIS MIDCOM)
  - terminal extensions
- Early stage
  - 3 Internet drafts from Cisco, NEC, Siemens
  - waiting for NTLP
Summary

• MIDCOM solutions are required for multimedia services across secure firewalls and NATs
• Three approaches are known:
  – ‘Call Agent’
    • MIDCOM MIB
    • Simple Middlebox Control (SIMCO) protocol
  – Smart Middlebox
    • Self-configuring firewall modules
  – Path-Coupled Signaling
    • to be developed and standardized at the IETF
    • waiting for NTLP