Status of the CORBA Firewall Traversal RFP

Brian Niebuhr
Network Associates - NAI Labs

DOCsec 2001 - Annapolis, MD
Overview

• Problem Statement
• Initial Solution
• RFP Information
• Current Submission
• Questions
Problem Statement - Causes

- Server location transparency
  - Firewalls require a priori knowledge of protected resources
- Peer-to-peer communication model
  - Firewalls designed for client-server model
  - Hosts using Network Address Translation (NAT) can be servers
Problem Statement - Illustration

External Client → TCP Firewall → Proxy Firewall → CORBA Servers → Internal Client

HTTP Server

CORBA Servers

Public Enclave

Private Enclave
Problem Statement - Illustration
Problem Statement - Definition

• Routing Problem
  – Large numbers of dynamic servers
  – Servers using NAT
  – Combinations of transport and application firewalls

• Policy Problem
  – Large numbers of dynamic servers
  – Non-traditional hosts as servers (e.g. callbacks)
Current Specification

- IOR contains firewall information
- Client invokes server-side proxy object to establish connections
- NORMAL and PASSTHRU connections
- Similar invocation to enable callbacks
- Bi-directional GIOP introduced for callbacks
Current Specification - Problems

• Proxified Object References
  – No definition of proxy object lifecycle
  – Proxy can’t map PASSTHRU connections to the correct target

• Callback Invocations
  – Client cannot know when to make new_callback() invocation
  – Only in specific firewall configurations
  – Third-party callbacks
Current Specification - Problems

- Bi-directional GIOP
  - Underspecified policies
  - Tied to transport-specific values
    - No mapping from transport endpoints to objects
    - Transport values sometimes unavailable
RFP Information

• New RFP issued last September
• Initial submissions presented in February
  – One joint initial submission by Borland, IBM, Iona, Sun, and Xtradyne, supported by Network Associates
• Revised submissions to be presented in July
• Vote on submission in November
Current Submission - Goals

• Uniform connection establishment
  – All GIOP versions
  – Various firewall topologies
  – Various firewall types
  – Various SSL connection termination points
  – Use of NAT

• Limit required ORB interaction with firewall to protocol inspection
Current Submission - Overview

• Many ideas taken from current specification
  – IOR contains firewall path information
  – Connection setup algorithm similar to the use of GIOP 1.2 profile addressing mode
  – Use of bi-directional GIOP for callbacks
• Uses connection setup message to establish connections
• Connection setup transparent to application
Current Submission - Details

- Host Identifiers describe the endpoints on a host
- Endpoints provide IIOP, NORMAL_SSL, or PASSTHROUGH services

<table>
<thead>
<tr>
<th>HID: 10.1.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>683: IIOP</td>
</tr>
<tr>
<td>684: SSL</td>
</tr>
<tr>
<td>684: PASSTHROUGH</td>
</tr>
</tbody>
</table>
Current Submission - Details

- Firewall Tagged Component
  - Contains an ordered list of Host Ids from the outermost-inbound firewall to the server
  - Multiple components indicate multiple paths

Firewall IOR Component:

<table>
<thead>
<tr>
<th>HID: 10.1.1.1</th>
<th>HID: 10.1.1.2</th>
<th>HID: 10.1.1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>683: IIOP</td>
<td>683: IIOP</td>
<td>683: IIOP</td>
</tr>
<tr>
<td>684: SSL</td>
<td>684: PASSTHRU</td>
<td>684: SSL</td>
</tr>
<tr>
<td>684: PASSTHRU</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Current Submission - Details

• Firewall Service Context
  – Indicates the path selected by the client
  – Contains the same ordered list of Host Ids with one endpoint selected from each

<table>
<thead>
<tr>
<th>HID: 10.1.1.1</th>
<th>HID: 10.1.1.2</th>
<th>HID: 10.1.1.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>684: SSL</td>
<td>683: IIOP</td>
<td>683: IIOP</td>
</tr>
</tbody>
</table>
Current Submission - Details

• Path selection policy
  – Determines which endpoints are chosen from each Host Id
  – Policy examples:
    • NO_SSL
    • GATEWAY_SSL
    • END_TO_END_SSL
• Configuration is implementation-dependent
Current Submission - Algorithm

Client ORB detects firewall component

Client (A) → Proxy Firewall (B) → Internet → TCP Firewall (W) → Proxy Firewall (X) → TCP Firewall (Y) → Server (Z)

IOR:
- W: SSL: 684, PASS: 684
- Y: IIOP: 683
- Z: IIOP: 683

Internet Servers (DNS, HTTP, etc.)

Status of the CORBA Firewall RFP - DOC sec 2001
Current Submission - Algorithm

Client ORB builds service context based on path selection policy

Client (A)  Proxy Firewall (B)  Internet  TCP Firewall (W)  Proxy Firewall (X)  TCP Firewall (Y)  Server (Z)

W:684/SSL  Y:683/IIOP  Z:683/IIOP

IOR:

W
SSL: 684
PASS: 684

Y
IIOP: 683
SSL: 684
PASS: 684

Z
IIOP: 683
SSL: 684

Internet Servers (DNS, HTTP, etc.)
Current Submission - Algorithm

Client ORB connects to client-side proxy and sends message

Client (A) → Proxy Firewall (B) → Internet → TCP Firewall (W) → Proxy Firewall (X) → TCP Firewall (Y) → Server (Z)


Internet Servers (DNS, HTTP, etc.)

Status of the CORBA Firewall RFP - DOC sec 2001
Current Submission - Algorithm

Client-side proxy determines target and forwards message

- **Client (A)**
- **Proxy Firewall (B)**
- **Internet**
- **TCP Firewall (W)**
- **Proxy Firewall (X)**
- **TCP Firewall (Y)**
- **Server (Z)**

**IOR:**
- **W**: SSL: 684, PASS: 684
- **Y**: SSL: 683, IIOP: 683
- **Z**: IIOP: 683

**Internet Servers (DNS, HTTP, etc.):**
- **W:684/SSL**
- **Y:683/IIOP**
- **Z:683/IIOP**
Current Submission - Algorithm

Server-side proxy observes which endpoints were chosen

Client (A)  Proxy Firewall (B)  Internet  TCP Firewall (W)  Proxy Firewall (X)  TCP Firewall (Y)  Server (Z)

<table>
<thead>
<tr>
<th>IOR:</th>
<th>W</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>683</td>
<td>683</td>
<td>683</td>
</tr>
<tr>
<td>IIOP</td>
<td>683</td>
<td>IIOP: 683</td>
<td>IIOP: 683</td>
</tr>
<tr>
<td>PASS</td>
<td>684</td>
<td>SSL: 684</td>
<td>SSL: 684</td>
</tr>
</tbody>
</table>

Internet Servers (DNS, HTTP, etc.)
Current Submission - Algorithm

Server-side proxy sends a reply

<table>
<thead>
<tr>
<th>IOR:</th>
<th>W</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SSL: 684</td>
<td>IIOP: 683</td>
<td>IIOP: 683</td>
</tr>
<tr>
<td></td>
<td>PASS: 684</td>
<td>SSL: 684</td>
<td>SSL: 684</td>
</tr>
</tbody>
</table>

Internet Servers (DNS, HTTP, etc.)

Status of the CORBA Firewall RFP - DOC sec 2001
Current Submission - Algorithm

SSL connection is established

Client (A) → Proxy Firewall (B) → SSL Internet → TCP Firewall (W) → Proxy Firewall (X) → TCP Firewall (Y) → Server (Z)

<table>
<thead>
<tr>
<th>IOR:</th>
<th>W</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>684</td>
<td>683</td>
<td>684</td>
</tr>
<tr>
<td>SSL</td>
<td>684</td>
<td>683</td>
<td>684</td>
</tr>
<tr>
<td>SSL</td>
<td>684</td>
<td>683</td>
<td>684</td>
</tr>
</tbody>
</table>

Internet Servers (DNS, HTTP, etc.)
Current Submission - Algorithm

Normal GIOP communication occurs
Current Submission - Details

• Callbacks
  – Routing problem solved like server-side invocations
  – Policy problem
    • Bi-directional GIOP for server-to-client invocations
    • Third-party callbacks must be avoided

• Delegated Identity
  – A trusted firewall can present the identity of the client or server for NORMAL_SSL connections
Current Submission - Details

• Access Control
  – Lightweight access control based on MDI
    • MDI provided by server ORB in the IOR
    • Client sends MDI in request message
  – MDI must be verified by the server ORB before performing request

• Dynamic Port Administration
  – Alternative solution based on dynamic configuration of the firewall
Summary

• New RFP issued to address problems with the CORBA firewall specification

• Goals of current submission
  – Uniform connection setup
  – Limit ORB interaction with firewall

• Current submission provides transparent connection setup via ORB invocation on target object
Questions?

- Contact Information:
  Brian Niebuhr
  bniebuhr@nai.com