1
Introdução

O padrão CORBA [1] [2] [3] surgiu na década de 90 com o propósito de oferecer aos desenvolvedores de aplicações distribuídas, orientadas a objetos, uma redução da complexidade no seus desenvolvimentos, entre outras vantagens. Questões como transparência de localização, protocolos de comunicação, conversão de tipos de dados em sequências de bits para transmissão, entre outras, foram abordadas por este padrão, liberando assim o desenvolvedor para se concentrar na aplicação a ser desenvolvida.

Paralelamente a esse desenvolvimento, a Internet presenciou um crescimento vertiginoso no número de usuários, o que entre outras coisas teve como consequência um maior número de ataques às redes internas[1]. Assim tiveram de ser desenvolvidas medidas mais severas para proteger essas últimas . Uma dessas medidas foi a utilização de *firewalls*. Firewalls são elementos de hardware ou software que protegem uma rede local de invasores externos [4]. O princípio que rege esses elementos é que qualquer pacote de rede que tente entrar ou sair da rede interna é examinado pelo firewall, que decide qual pacote será repassado (para a rede interna ou externa) utilizando regras previamente configuradas.

Firewalls e CORBA podem coexistir até agora sem grandes impedimentos, contanto que as aplicações funcionem dentro de um mesmo domínio administrativo de rede. Problemas surgem quando é necessário atravessar as fronteiras desses domínios. Os principais problemas são devidos, essencialmente, a duas grandes características de CORBA [5]: transparência de localização de servidores e modelo de comunicação baseado em pares.

O primeiro diz respeito ao fato dos clientes de um objeto CORBA não precisarem saber explicitamente da sua localização exata para realizarem

[1]Neste trabalho por "rede interna" entende-se uma rede local que eventualmente precisa ser protegida enquanto que "rede externa" denota o ambiente externo no qual esta rede está inserida.

uma invocação remota. Esses objetos podem, assim, mudar de endereço (de máquina) sem que isso implique em problemas para os seus clientes (desde que algumas condições sejam satifeitas). Apesar da flexibilidade oferecida no desacoplamento entre clientes e servidores poder ser vista como uma vantagem, na presença de um firewall, isso pode acarretar graves problemas para a aplicação e para a administração da rede. Os firewalls geralmente controlam o acesso aos servidores através da liberação de conexões destinadas a endereços e portas específicos (endereços e portas dos servidores). Para que requisições a objetos CORBA possam atravessar as fronteiras da rede, a cada mudança de endereço destes objetos, não apenas os serviços CORBA de infra-estrutura (serviço de nomes por exemplo) devem ser notificados, mas também as regras do firewall têm que ser atualizadasi, a fim de manter a permissão de travessia. Em um ambiente com poucos objetos servidores, que por sua vez tenham uma frequência de mobilidade baixa, este problema pode até ser desconsiderado. No entanto, como será visto adiante, aplicações CORBA de grande porte se caracterizam por oferecer serviços através de um elevado número de objetos, cuja mobilidade é suficiente para levar em consideração este problema (entenda-se aqui por mobilidade a mudança de endereço IP e/ou porta).

O modelo de comunicação baseado em pares também entra em conflito com a presença de firewalls, uma vez que uma de suas principais características é a existência de um número muito grande de servidores (qualquer elemento pode ser potencialmente tanto um cliente como um servidor), o que acarreta um número excessivo de regras. Este fato traz como consequência uma grande dificuldade na manutenção dessas regras, além de reduzir a eficiência do firewall na comunicação das aplicações.

Outro problema com a travessia de redes por comunicação CORBA surge quando a rede interna utiliza o serviço NAT [2]. Esse serviço tem como principais objetivos a possibilidade de criação de um espaço de endereçamento privado e a ocultação da topologia da rede interna perante o ambiente exterior. Os endereços NAT (endereços IP 10.x.x.x, 172.16.x.x e 192.168.x.x) são usados internamente e não podem ser utilizados na rede externa (Internet). Para que os nós da rede interna possam se comunicar externamente, existe um elemento (geralmente o próprio firewall) que é responsável por traduzir esses endereços para endereços válidos (endereços IP roteáveis que podem ser alcançados por qualquer elemento da rede externa, utilizando apenas o protocolo de roteamento IP). Assim, é possível que todas as estações de uma rede interna

[2] *Network Address Translation* - Tradução de endereços de rede.

compartilhem, de maneira mais eficiente, os endereços IP roteáveis disponíveis para a rede.

O problema com este serviço surge quando um objeto CORBA que reside em uma rede com NAT exporta seu endereço/porta IP no perfil IIOP [6] do IOR [3]. O endereço contido ali não tem nenhum significado fora da rede interna e, portanto, nenhum cliente externo conseguirá se conectar com o objeto CORBA. Uma solução trivial para esse problema seria alocar para cada estação que hospedasse objetos CORBA um endereço IP roteável. No entanto, essa solução não é escalável quando muitas estações passarem a hospedar esses objetos.

Conforme foi apresentado anteriormente, existem problemas na coexistência entre aplicações CORBA, firewalls e NAT, no momento em que as primeiras necessitem atravessar as fronteiras da rede interna. Este trabalho tem como objetivo apresentar soluções para a travessia de firewalls/NAT por parte das aplicações que utilizem CORBA como platafoma de comunicação. As soluções apresentadas devem obedecer aos seguintes requisitos:

- A administração do firewall/NAT não deve ser sobrecarregada. Se possível não deve requerer nenhuma configuração;
- Tanto quanto possível, deve ser de fácil configuração e transparente para o desenvolvedor de aplicações;
- Não deve impor excessivo impacto negativo no desempenho das aplicações.

Três soluções para abordar este problema são apresentadas e avaliadas por este trabalho, onde cada uma é destinada a uma configuração específica de firewall e requer um grau diferente de configuração da aplicação. O motivo de se desenvolver diferentes soluções é aproveitar características específicas de cada cenário (como por exemplo a possibilidade de abertura de conexões TCP para fora da rede interna), a fim de se reduzir o impacto no desempenho das aplicações.

O restante do texto está organizado da seguinte forma: o Capítulo 2 irá apresentar os trabalhos relacionados à travessia de firewalls por aplicações distribuídas que influenciaram a realização deste trabalho; o Capítulo 3 descreve as três propostas de travessia de firewalls/NAT desenvolvidas neste trabalho, enquanto que o Capítulo 4 relata detalhes importantes na implementação das

[3] *Interoperable Object Reference - Referência ao objeto CORBA*

soluções propostas; o Capítulo 5 apresenta os diversos testes realizados para validar as soluções propostas e, por fim, Capítulo 6 relata algumas conclusões obtidas com este trabalho e algumas sugetões de trabalhos futuros.