UNIVERSIDADE REGIONAL DE BLUMENAU

CENTRO DE CIÊNCIAS EXATAS E NATURAIS

CURSO DE SISTEMAS DE INFORMAÇÃO – BACHARELADO

SISTEMA DE CONTROLE DE ACESSO DE NOTEBOOKS, DESKTOPS E ATIVOS DE REDE EM UMA LAN

DAVID KRZIZANOWSKI

BLUMENAU
2006

2006/1-XX

DAVID KRZIZANOWSKI

SISTEMA DE CONTROLE DE ACESSO DE NOTEBOOKS, DESKTOPS E ATIVOS DE REDE EM UMA LAN

Trabalho de Conclusão de Curso submetido à Universidade Regional de Blumenau para a obtenção dos créditos na disciplina Trabalho de Conclusão de Curso II do curso de Sistemas de Informação — Bacharelado.

Prof. Francisco Adell Péricas - Orientador

BLUMENAU
2006

2006/1-XX

SISTEMA DE CONTROLE DE ACESSO DE NOTEBOOKS, DESKTOPS E ATIVOS DE REDE EM UMA LAN

Por

DAVID KRZIZANOWSKI

Trabalho aprovado para obtenção dos créditos na disciplina de Trabalho de Conclusão de Curso II, pela banca examinadora formada por:

Presidente:	Prof. Francisco Adell Péricas, Mestre – Orientador, FURB
Membro:	Prof. Paulo Fernando da Silva, Mestre – FURB
Membro:	Prof. Sérgio Stringari, Mestre – FURB

Blumenau, 13 de julho de 2006

Dedico este trabalho a minha família principalmente a esposa e filho pela paciência e compreensão ao longo deste desafio.

AGRADECIMENTOS

À Deus, pelo seu imenso amor e graça.

À minha família, que esteve sempre ao meu lado.

Aos amigos que contribuíram de alguma forma para a conclusão deste trabalho.

Ao meu orientador, Francisco Adell Péricas pelo apoio durante a jornada da execução deste trabalho.

Se todos nós fizéssemos as coisas somos capazes, ficaríamos espantados conosco mesmos.

Thomas Edison

RESUMO

Este trabalho apresenta o desenvolvimento de um software para controle de acesso a redes de computadores, partindo do princípio que o invasor possa estar fisicamente dentro de uma empresa. É apresentado também um estudo das camadas do protocolo TCP/IP, de onde são extraídas informações para validação dos computadores que possuem permissão de comunicação.

Palavras-chave: Segurança. Gerenciamento. Controle.

ABSTRACT

This work presents the development of software for access control the computer networks, leaving of the principle that the invader possibility is physically inside of a company. A study of the layers of protocol TCP is also presented, of where information for validation of the computers are extracted that possess communication permission.

Key-words: Security. Management. Control.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ARP – Address Resolution Protocol

BCC – Curso de Ciências da Computação – Bacharelado

DHCP - *Dynamic Host Configuration Protocol*

DNS – *Domain Name System*

DSC – Departamento de Sistemas e Computação

FTP – *File Transfer Protocol*

HTTP – *Hypertext Transfer Protocol*

ICMP – *Internet Control Message Protocol*

IP – *Internet Protocol*

Ipv4 – *Internet Protocol version 4*

Ipv6 – *Internet Protocol version 6*

LAN – *Local Area Network*

MAC – *Media Access Control*

MAN – *Metropolitan Area Network*

SBC – Sociedade Brasileira de Computação

SMTP – *Simple Mail Transfer Protocol*

SP1 – *Service Pack 1*

SP2 – *Service Pack* 2

TCP – *Transmission Control Protocol*

UDP – *User Datagram Protocol*

WAN – *Wide Area Network*

SUMÁRIO

1 INTRODUÇÃO

Em um ambiente de informática corporativo que possui interligação com a rede mundial de computadores *(internet)*, é comum a existência de um sistema de segurança chamado *firewall*. De acordo com Torres (2001, p. 415), "Um *firewall* é, na realidade, um poderoso roteador interligando duas redes [...]. De um lado tem a rede pública, ou insegura e, do outro, a rede privada ou segura".

Utilizando uma analogia simplista, o sistema de *firewall* faz o papel de um vigia que se encontra no portão da empresa, deixando entrar ou sair somente pessoas autorizadas. Nesta forma de utilização de *firewall*, o sistema de segurança protege principalmente a rede *Local Area Network (*LAN*)* de ameaças advindas da internet.

No caso de uma possível ameaça se encontrar dentro da rede LAN, o sistema de *firewall* tradicional será ineficaz, pois ele estará protegendo somente a entrada e a saída para *internet*. Os computadores dos usuários não estarão protegidos de um possível ataque originado de um computador que se encontre fisicamente dentro de uma empresa. Isto permite que um equipamento não autorizado explore vulnerabilidades na rede LAN e na rede *Wide Area Network* (WAN) (RUBIN; CHESWICK; BELLOVIN, 2005).

Estes equipamentos não autorizados são na sua maioria computadores portáteis que podem ser conectados à rede LAN por funcionários, clientes, fornecedores ou visitantes. Existem duas formas destes equipamentos conseguirem acesso à rede: configurando o endereço do *Internet Protocol (*IP) de forma dinâmica fornecido pelo *Dynamic Host Configuration Protocol (DHCP*), ou utilizando um endereço IP estático (TORRES, 2001).

Algumas empresas utilizam a prática de configurar o DHCP para distribuir endereços somente para uma lista de endereços físicos da placa de rede *(MAC-address*) previamente aprovada. Esta solução não resolve o problema se o equipamento não autorizado estiver

configurado com um endereço IP estático (LOPES; SAUVÉ; NICOLLETTI, 2003).

Outra forma de bloquear a comunicação de equipamentos não autorizados é a utilização de chaves de autenticação privada, onde os computadores conseguem se comunicar apenas com os demais equipamentos que possuem a mesma chave (RUBIN;CHESWICK, 2001). Nesta solução, pode haver dificuldade, de integração e gerenciamento em uma empresa que possui ambiente operacional heterogêneo, utilizando sistemas operacionais diferentes como MS-Windows, HP-UX, AIX e Linux.

Existem dispositivos de rede utilizados para interligar os computadores em uma rede LAN, chamados *Switchs*, que são capazes de bloquear a comunicação de equipamentos que não possuem seu *MAC-address* liberado pelos administradores da rede. Este tipo de *Switch* seria a solução mais apropriada para eliminar o problema, porém seu alto custo de aquisição inviabiliza sua implementação na maioria das empresas.

Este trabalho irá demonstrar o processo de criação de uma solução de controle de acesso a uma rede LAN para a empresa Quick Soft Sistema de Informações Ltda. A solução consiste na utilização do *firewall* dos sistemas operacionais Windows XP SP2 e Windows 2003 Server SP1 localizados na rede LAN. Todos os *firewall*s internos da rede LAN serão gerenciados pelo sistema, que terá uma base de dados contendo uma lista de MAC-*addresses* conhecidos. Desta forma, será permitida a comunicação apenas entre os equipamentos que possuem seu endereço físico cadastrado e autorizado.

1.1 OBJETIVOS DO TRABALHO

O objetivo deste trabalho é a especificação e implementação de um sistema de controle de acesso a estações e servidores Windows em uma rede LAN através do gerenciamento de *firewalls* distribuídos.

Os objetivos específicos do trabalho são:

a) gerenciamento do *firewall* nativo do sistema operacional Windows XP SP2;

b) interceptação e interpretação de pacotes TCP/IP para o controle de acesso dos equipamentos de rede;

c) monitoração de atividades de bloqueio dos *firewalls*;

d) armazenamento de informações monitoradas.

1.2 ESTRUTURA DO TRABALHO

O capítulo 1 apresenta a estrutura geral do trabalho, a introdução, os objetivos que se quer alcançar a localização dos assuntos abordados e a organização do trabalho.

No capítulo 2 são apresentados os protocolos comumente usados em redes locais e internet, os principais riscos de seguranças de rede e a utilização de firewalls.

O capítulo 3 descreve o ambiente de informática da empresa no qual este software será implantado, descrição do desenvolvimento, apresentando os seus requisitos, a especificação através dos diagramas de classe, de atividades e de casos de uso. Também são apresentadas as suas funcionalidades e todo o esquema de funcionamento.

O capítulo 4 apresenta as conclusões sobre o trabalho e sugestões para extensões e trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Neste capítulo serão abordados os assuntos que servem de base para o entendimento da solução apresentada. Será apresentado um estudo sobre os protocolos usados comumente em redes locais e internet, os principais riscos de seguranças de rede e a utilização de *firewalls*.

2.1 CONJUNTO DE PROTOCOLOS TCP/IP

No final dos anos 60 o departamento de defesa norte americano (DoD) se interessou por um protocolo que estava sendo desenvolvido pelas universidades para interligação de seus sistemas computacionais. O principal objetivo era manter a comunicação com diversos sistemas distribuídos em vários países no caso de uma guerra nuclear. Desta parceria do governo com as universidades surgiu uma rede de quatro nós chamada de ARPANET, que mais tarde se transformaria em INTERNET. No final dos anos 70, esta rede inicial evoluiu, teve seu protocolo principal desenvolvido e transformado na base para o *Transmition Control Protocol / Internet Protocol* (TCP/IP) (GOMES, 2000).

O conjunto de protocolos denominado TCP/IP permite que diversos computadores de modelos e fabricantes diferentes, executando sistemas operacionais distintos, comuniquem entre si através da troca de pacotes de informação. Os protocolos estão devidamente organizados em uma estrutura de camadas, em que cada uma é responsável por uma parte da comunicação. Um conjunto de protocolos organizados em camadas lógicas origina uma pilha de protocolos, pelo que se conclui que a pilha de protocolos Internet representa a forma como se organizam logicamente os diversos protocolos comumente chamados por TCP/IP (KUROSE, 2001).

A pilha de protocolos Internet é composta de quatro camadas, cada uma com funções

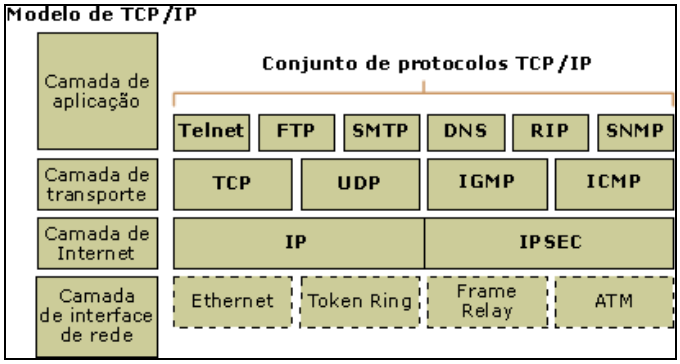
próprias (figura1):

a) camada de interface de rede – inclui os *softwares* de controle das interfaces de rede acoplados aos sistemas operacionais e aos correspondentes dispositivos físicos de interligação, podendo dizer-se que esta camada trata dos aspectos ligados aos equipamentos que utilizam o meio de comunicação (*Ethernet*, ATM, ADSL, etc);

b) camada de internet – gerencia a transferência dos pacotes de informação na rede, incluindo-se nesta camada os mecanismos do seu encaminhamento. Alguns dos protocolos da pilha Internet que são manipulados nesta camada são o *Internet Protocol (IP*) e o *Internet Control Message Protocol* (ICMP);

c) camada de transporte – fornece controles de fluxo de dados entre dois computadores, essencialmente através dos protocolos de transporte *User Datagram Protocol (UDP*) sem conexão e *Transmission Control Protocol (TCP*) orientado a conexão;

d) camada de aplicação – a camada de aplicação é a camada que a maioria dos programas de rede usa de forma a se comunicarem através de uma rede com outros programas: protocolo para acesso remoto (TELNET), *File Transfer Protocol (*FTP), *Simple Mail Transfer Protocol (SMTP*) e *Hypertext Transfer Protocol* (HTTP).



Fonte: Microsoft (2000)

Figura 1 – Modelo TCP e suas camadas

2.1.1 ENDEREÇOS DE REDE

Cada interface de rede que use a pilha de protocolos Internet necessita de uma identificação única para seu correto funcionamento. Existem dois sistemas de endereçamento de rede:

a) IPv4 - endereços são definidos por 32bits;

b) IPv6 - endereços são definidos por 128bits.

Os endereços de IPv4 são organizados em classes de endereçamento que permitem definir redes de diferentes dimensões:

a) Classe A: bit ‘0’ + 7bits de rede + 24bits da interface.

   Dimensões: de 1.0.0.0 a 126.255.255.255

b) Classe B: bits ‘10’ + 14bits de rede + 16bits da interface.

   Dimensões: de 128.0.0.0 a 191.255.255.255

c) Classe C: bits ‘110’ + 21bits de rede + 8bits da interface.

   Dimensões: 192.0.0.0 a 223.255.255.255

*Unicas*t é uma tecnologia que permite o envio de pacotes de uma computador diretamente a outro, e mesmo no endereçamento IPv6 onde não existe o conceito de classes de endereços, a função de seus endereços *unicast* é exatamente a mesma do IPv4.

Com o objetivo de facilitar a comunicação entre os computadores, desenvolveu-se um sistema de identificação de interfaces de rede através de nomes. Esse sistema de nomeação de interfaces e computadores denomina-se *Domain Name System (*DNS).

O DNS é um esquema de gerenciamento de nomes, hierárquico e distribuído, que define a sintaxe dos nomes usados nas redes de computadores, regras para delegação de autoridade na definição de nomes, um banco de dados distribuído que associa nomes a atributos (entre eles o endereço IP) e um algoritmo distribuído para mapear nomes em

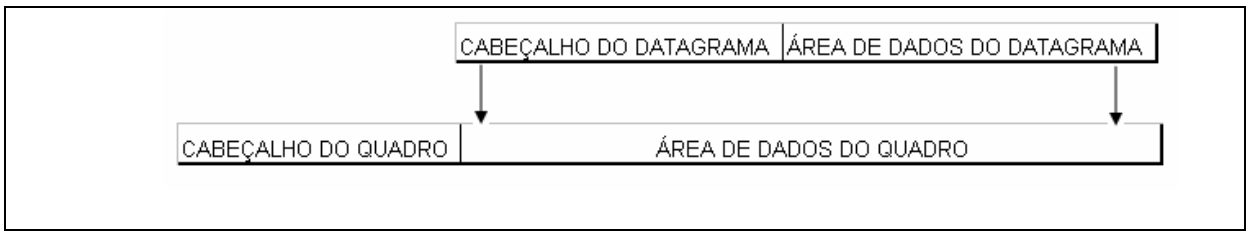
endereços.

2.1.2 TRANSMISSSÃO DE INFORMAÇÕES NA CAMADA APLICAÇÃO

Para transmitir informações de uma aplicação origem para uma aplicação destino, é utilizado o processo de encapsulamento de informações nas camadas lógicas nas quais se definem protocolos de comunicação. A forma encontrada para fazer circular a informação entre a aplicação emissora através da rede até a aplicação receptora baseia-se no encapsulamento sucessivo dos dados em pacotes de informação (COMER, 1998).

O processo é construído de um novo pacote adicionando um cabeçalho adequado ao pacote do protocolo anterior (Figura 2). No computador destinatário é executado o processo inverso (remoção de cabeçalhos) até se restituir todos os dados à sua forma original e entregue à aplicação destino.

Durante a travessia na rede, os dados circulam em pacotes cujo formato depende dos meios físicos usados, mas contém todo o encapsulamento efetuado no emissor. Os dispositivos de interligação de redes podem assim observar os pacotes em trânsito e tomar decisões de encaminhamento baseando-se nos cabeçalhos desses pacotes.



Fonte: Comer (1998)

Figura 2 – Encapsulamento de dados

A grande maioria das aplicações de rede é estruturada em modo cliente/servidor, onde existe um servidor com uma aplicação ativa aguardando informações em uma determinada porta da rede. Esta aplicação poderá atuar em modo iterativo ou concorrente, onde a principal diferença entre as duas é que no modo concorrente é possível atender várias conexões de origens distintas.

Os servidores de aplicação são tipicamente associados a portas UDP ou TCP pré-definidas, utilizando portas de rede que variam entre 0 a 65535. No lado cliente, as portas utilizadas tendem a ser “aleatoriamente” escolhidas e a permanecer ativas apenas durante a execução do serviço. A escolha da porta usada na parte cliente geralmente é escolhida pela pilha de protocolos Internet em junção com o sistema operacional.

2.1.3 PROTOCOLO IP

Segundo Comer (1998), o *Internet Protocol* (IP) especifica o formato de pacotes de interligação em redes denominados datagramas e inclui formalmente as idéias de transmissão sem conexão. A ausência de conectividade indica que o protocolo IP não possui nenhum controle sobre o estado ou contexto dos sucessivos pacotes que processa, e a não confiabilidade está na limitação de não conseguir garantir que os pacotes processados chegam ao seu destino.

Quando um pacote não chega ao seu destino, o tratamento de erro do protocolo IP consiste em ignorar o pacote e tentar enviar uma mensagem informativa do tipo ICMP para a entidade que originou esse pacote.

Como apresentado anteriormente, o endereço Ipv4 é composto de 4 octetos, que são divididos em uma parte de rede e uma parte de dispositivo, chamados de identificadores de rede e de *host*, de acordo com o tipo de classe definido pelos primeiros bits do primeiro

octeto, e/ou subrede, definida pelo número de máscara de sub-rede.

Este protocolo, usando a parte de rede do endereço ou identificador de rede, pode definir a melhor rota através de uma tabela de roteamento mantida e atualizada pelos roteadores.

O protocolo recebe os dados da camada superior (transporte) na forma de segmentos. Ocorre então o processo de fragmentação e os conjuntos de dados passam a se chamar datagramas. Estes datagramas são então codificados para envio à camada inferior (física) para encaminhamento no meio físico.

A figura 3 relaciona as nove partes que constituem um datagrama, o número de bits e função ou descrição de cada uma delas.

<table>
<tr><td>VERS</td><td>HLEN</td><td>TIPO DE SERVIÇO</td><td colspan="2">COMPRIMENTO TOTAL</td></tr>
<tr><td colspan="3">IDENTIFICAÇÃO</td><td>FLAGS</td><td>DESLOCAMENTO DO FRAGMENTO</td></tr>
<tr><td>TEMPO DE VIDA</td><td>PROTOCOLO</td><td colspan="3">VERIFICAÇÃO DA SOMA DO CABEÇALHO</td></tr>
<tr><td colspan="5">ENDEREÇO IP DE ORIGEM</td></tr>
<tr><td colspan="5">ENDEREÇO IP DE DESTINO</td></tr>
<tr><td colspan="4">OPÇÕES IP (SE HOUVER)</td><td>PADDING</td></tr>
<tr><td colspan="5">DADOS</td></tr>
<tr><td colspan="5">. . .</td></tr>
</table>

Fonte: Comer (1998)

Figura 3 – Datagrama do protocolo IP

A primeira parte (VERS) é o cabeçalho que contém informação sobre a versão do número IP (IPv4 ou IPv6) e o tipo de serviço (ToS), muito usado em aplicações que necessitem de Qualidade de Serviço (QoS).

A segunda parte (HLEN), comprimento informa o comprimento do datagrama incluindo dados e cabeçalho.

A terceira parte (IDENTIFICAÇÃO, FLAGS e DESLOCAMENTO DE FRAGMENTO), fragmentação, instrui ao protocolo, como reagrupar datagramas quando chegam após um processo de fragmentação muito comum em interfaces defeituosas e tráfego intenso.

A quarta parte (TEMPO DE VIDA), informa o número de roteadores que podem redirecionar o datagrama. O valor é decrementado até zero a cada roteador quando então o datagrama é descartado, impedindo a criação de *loops* e assim garantindo estabilidade ao processo de roteamento.

A quinta parte (PROTOCOLO) informa qual protocolo deverá receber o datagrama na próxima camada. Se o valor deste campo for 6, TCP, se 7, UDP.

A sexta parte (SOMA DE VERIFICAÇÃO DO CABEÇALHO) assegura a integridade dos valores do cabeçalho.

Os próximos campos, sétimo e oitavo, (ENDEREÇO IP ORIGEM e DESTINO), 32 bits cada, caracterizam por completo toda informação sobre endereçamento necessária ao processo de roteamento.

O último campo contém os dados, a informação na realidade, e tem tamanho livre, porém definido pelo tipo de rede, sendo o máximo possível de 1500 bytes.

Todas as informações necessárias para que o IP possa se comunicar com o resto da rede estão distribuídas nestes campos, principalmente naqueles relativos ao endereçamento. É importante observar que a camada de rede utiliza estes endereços lógicos de 4x8bits, para definir as redes existentes e como conseguir obter informação delas. Entretanto, para que os dados cheguem aos *hosts* é necessário o endereço *Media Access Control* (MAC).

O TCP/IP define um protocolo, *Address Translation Protocol* (ARP), que caracteriza e relação entre o endereço IP e o endereço MAC.

2.1.4 PROTOCOLO ARP

Segundo Comer (1998), o *Address Resolution Protocol* (ARP) executa a conversão de endereço dinâmica, usando somente o sistema de comunicação de rede de baixo nível. ARP

permite que os computadores convertam endereços sem manter um registro permanente das vinculações.

Na construção do datagrama, a aplicação conhece os endereços MAC e IP do computador origem e somente o endereço IP do computador destino. Para descobrir o endereço MAC de computador destino, o protocolo ARP envia uma consulta na rede para todos os dispositivos do segmento perguntando qual computador possui o IP destino sobre seu endereço MAC. O computador destino responderá diretamente ao computador origem daquele segmento informando seu endereço físico, sem utilizar transmissão por difusão. O computador origem irá armazenar o endereço MAC temporariamente na sua tabela ARP (IPxMAC), também chamada de *proxycache* ARP. Após obter todas as informações necessárias, o dispositivo origem envia o quadro (*frame*) para seu destino.

Neste exemplo o mesmo quadro é enviado para o destino e também para a interface do roteador deste segmento, porém somente o dispositivo destino irá abrir o quadro até a última camada pois somente ele tem o endereço MAC destino.

2.1.5 PROTOCOLO ICMP

Comer (1998) indica que o ICMP é um protocolo de mensagens de controle usado basicamente para três funcionalidades: avisar quando o fluxo de mensagens é maior que a capacidade de processamento de um dispositivo; checar o número de roteadores que o pacote já percorreu (parâmetro *Time To Live* (TTL)); e mensagens de redirecionamento.

Eventualmente um roteador pode estar recebendo mais informação do que pode processar, sendo assim ele passa a contar com controle de fluxo, enviando uma mensagem *source quench* para o dispositivo origem para que ele pare ou diminua o fluxo de dados.

O segundo caso envolve o parâmetro TTL do cabeçalho do pacote IP que basicamente

é o número de roteadores ou *hops* total que uma informação pode percorrer. Ele é decrementado a cada *hop* e quando chega a zero, o roteador descarta o datagrama e envia uma mensagem à fonte informando que a informação não chegou ao seu destino, utilizando o ICMP.

O terceiro caso é a mensagem de redirecionamento ICMP, que é utilizada quando o roteador determina que um caminho melhor existe para o pacote que acabou de ser enviado assim mesmo. Neste caso a implementação do protocolo de roteamento pode definir um novo caminho.

2.1.6 REDES LAN, MAN E WAN

As redes LAN emergiram para possibilitar o compartilhamento de recursos (Hardware e Software) e de informações, bem como a troca de informações entre vários computadores, mantendo a independência entre as diversas estações de trabalho conectadas à rede e possibilitando a integração destas estações e seus recursos em ambientes de trabalho corporativos (SOARES; LEMOS; COLCHER, 1995).

Uma rede LAN é limitada em uma pequena região, onde sua principal característica é não necessitar do uso de telecomunicações como meio de transmissão de dados entre seus nós, que correspondem aos próprios computadores dos usuários.

Entre as características básicas das redes LANs, segundo Soares, Lemos e Colcher (1995), estão:

a) abrangência geográfica limitada (distâncias menores que 25 km);

b) altas taxas de transmissão;

c) baixas taxas de erro;

d) pequenos atrasos de transmissão;

e) geralmente redes privadas;

f) facilidade de interconexão entre redes distintas.

As redes MAN possuem características similares a rede LAN, diferenciando-se por cobrir uma área física maior. Uma rede MAN pode abranger uma área de uma cidade (SOARES; LEMOS; COLCHER, 1995).

Segundo Soares, Lemos e Colcher (1995), as redes WAN são as pioneiras entre as redes de computadores. São constituídas de uma diversidade de aplicações e usos, destacando-se as redes públicas, isto é, “o sistema de comunicação é mantido, gerenciado e de propriedade de grandes operadoras (públicas ou privadas) e seu acesso é público”.

As redes WAN possuem um custo elevado de comunicação, por isto a taxa de transmissão é baixa, mesmo que hoje em dia alguns *links* alcancem a velocidade de megabits por segundo (Mbps).

2.2 RISCOS DE SEGURANÇA DE UMA REDE DE COMPUTADORES

Segundo Rubin e Cheswick (2001), os riscos de segurança dos computadores estão concentrados em perdas de dados, confidencialidade, privacidade e disponibilidade de recursos.

Em um incidente de falha de segurança, o mais comum é ocorrer eliminação ou modificação de informações. Ataques destrutivos geralmente ocorrem através da execução de programas que possuem privilégios adicionais obtendo acesso aos dados.

A detecção de uma falha de segurança pode levar muito tempo, tornando sua restauração cada vez mais cara ou até inviável. Dependendo do tempo que passou entre o ataque e sua detecção, as informações restauradas de *backup* poderiam gerar um impacto no sistema sendo mais viável regerá-las.

Uma das principais causas de perda de confidencialidade é a negligência quanto à divulgação de informações. Nas estações dos usuários podem ser encontradas informações financeiras estratégicas, novos projetos, e-mails importantes, lista de senhas e outros documentos que não poderiam ser entregues a pessoas erradas.

Comumente os computadores dos usuários são pouco seguros, contendo compartilhamento de seus arquivos através de senhas consideradas fracas ou óbvias. Ataques à computadores são realizados através de códigos maliciosos que obtém controle da estação, extraindo seus dados para fora da empresa sem que um usuário comum consiga detectá-lo.

A questão privacidade está muito próxima a da confidencialidade, porém a privacidade está mais relacionada ao perfil do usuário, o que ele faz, suas preferências, e outras características. Estas informações são preciosas nas mãos de pessoas especializadas em levantar perfil de pessoas e revender para empresas comerciais.

Outro tipo de ataque são os voltados para a interrupção de recursos fundamentais a um a rede de computadores como, por exemplo, servidores de e-mail, páginas *WEB* e banco de dados. Ataques desta natureza são voltados para as vulnerabilidades do serviço escolhido, fazendo com que este se torne indisponível, gerando prejuízos aos seus fornecedores e clientes.

Rubin e Cheswick (2001) acrescenta que as principais causas para as vulnerabilidades dos computadores estão relacionadas às falhas na construção dos programas, popularmente conhecidas como *bugs*, administração da rede inadequada e usuários descuidados ou mal treinados.

Os usuários muitas vezes são culpados pelas perdas de segurança de seus dados, porém o que se observa é falta de informação e treinamento apropriado para os usuários finais adicionado a sistemas complexos e sem prática de manuseio.

A relação segurança versus flexibilidade é inversamente proporcional, ou seja, quanto

mais seguro o ambiente, menos acessos o usuário terá. É preciso realizar um forte trabalho de educação e persuasão para demonstrar aos usuários que as políticas de segurança devem ser praticadas para proteger seus dados.

A qualidade da administração de uma rede de computadores é um dos mais importantes fatores na segurança de uma empresa. A configuração de *firewalls*, detecção de intrusos através de *Intrusion Detection System* (IDS), configuração de autenticação da rede com políticas de senhas consideradas fortes, políticas de acesso a internet, políticas de proteção às estações e atualização constante dos sistemas são algumas das atividades básicas do administrador da rede.

2.3 FIREWALL

O *firewall* pode ser definido como um sistema de segurança disposto entre duas redes de comunicação que possui as seguintes propriedades: todo o tráfego de dentro para fora dessa rede e vice-versa deve passar pelo *firewall*. Só o tráfego definido pela política de segurança da rede é permitido a passar pelo *firewall*.

Rubin e Cheswick (2001) indica que há dois tipos básicos de *firewall*. O primeiro é o de aplicação por *gateway*, também conhecido por PROXY, que reconstrói os dados das aplicações e utiliza informações internas dos pacotes para permitir ou negar o tráfego. Este método é utilizando principalmente para controlar a navegação de sites da internet. O segundo é o filtro de pacotes: é o modo mais comum utilizado, onde são examinados os datagramas do protocolo IP que entram e saem da rede. Para cada pacote é tomada uma decisão de permitir que este chegue ao seu destino ou descartado.

Principais parâmetros para o filtro de pacotes:

a) IP origem – indica o endereço de rede de um ou mais computadores que gerou o

pacote. É usado para controlar a entrada ou saída de pacotes de uma determinada faixa de endereços.

b) IP destino – indica o endereço de rede de um ou mais computadores de destino do pacote. Também usado para controlar a entrada ou saída de pacotes de uma determinada faixa de endereços.

c) Portas – indica a porta utilizada no pacote no qual está associada a algum serviço. Com esta regra é possível, por exemplo, bloquear a entrada de pacotes da porta 23 (telnet) cujo as informações não são criptografadas.

d) Protocolo – indica o tipo de protocolo que será controlado. Exemplos TCP e UDP.

Uma outra forma de uso de *firewall* é o distribuído, geralmente chamado de *firewall* pessoal, que pode ajudar a evitar que invasores e softwares mal intencionados encontrados na rede comprometam seus sistemas de computadores. O uso dessa tecnologia é importante para evitar que usuários remotos ou móveis transmitam programas maliciosos involuntariamente. *Firewalls* distribuídos são *firewalls* instalados individualmente em cada computador, cujas regras implementadas são centralizadas em um computador da rede. Dependendo do software escolhido, um *firewall* pessoal pode oferecer recursos além daqueles oferecidos pelos *firewalls* da rede, como proteger computadores contra software chamados de espiões e cavalos de Tróia.

3 DESENVOLVIMENTO DO TRABALHO

Neste capítulo será demonstrado o detalhamento do ambiente de informática da empresa Quick Soft , onde será implantado o sistema. Serão demonstradas as funcionalidades do software, sua especificação através de *Unified Modeling Language* (UML), requisitos, ferramentas de desenvolvimento utilizadas e resultados.

3.1 REDE DE COMPUTADORES DA QUICK SOFT

Atualmente a rede de computadores da Quick Soft é formada por aproximadamente 80 estações de trabalho e 15 servidores Microsoft Windows e 10 servidores Linux Red Hat, atendendo os serviços de *Firewall*, Proxy, E-mail, banco de dados, autenticação de rede, arquivos, *Domain Name Service* (DNS), Dynamic *Host Configuration Protocol* (DHCP), terminais, gerenciamento de antivírus, gerenciamento de circuito interno de TV, *backups*, páginas *WEB* e outros.

A proteção da rede LAN é feita por dois servidores *firewall* configurados em modo de alta disponibilidade, ou seja, se um deles tornar-se indisponível o segundo continua atendendo todas as funcionalidades do primeiro. Nos demais serviços fundamentais como autenticação de rede, banco de dados e servidores de terminais também existe alta disponibilidade ou contingência para contorno de inoperabilidade.

Todas as estações e servidores estão protegidos por um sistema de antivírus corporativo, cujo gerenciamento é centralizado por um servidor.

As estações e servidores Microsoft Windows estão configuradas para a atualização automática de correções críticas enviadas pelo fornecedor. Outros tipos de atualizações são efetuados após prévia avaliação. Os servidores Linux recebem constantes atualizações de

segurança, porém em modo manual.

São utilizadas políticas de grupos nas estações e servidores de terminais pertencentes a domínio Microsoft para limitar os privilégios dos usuários comuns, impedindo acessos às configurações administrativas dos computadores, impedindo a navegação na rede interna, e outras atividades que pudessem explorar algum tipo de vulnerabilidade.

O sistema de e-mail é protegido por antivírus, antispam e por filtros com vários tipos de regras para controlar a entrada e saída de informações. Todos os e-mails de entrada ou saída podem ser auditados.

O sistema de mensagem instantânea utilizado possui bloqueios de tráfego de arquivos, controle sobre os contatos utilizados e auditoria de todos os diálogos.

Devido ao grande volume de pessoas entrando e saindo da empresa com computadores móveis, surgiu a necessidade do controle de acesso deste tipo de equipamento. Estas pessoas são funcionários, clientes, fornecedores e visitantes que por determinadas circunstâncias necessitam de acesso à rede local.

Os *notebooks* na sua maioria são equipamentos particulares, que freqüentemente são conectados diretamente à *internet* sem proteção de um *firewall* e um sistema eficaz contra *softwares* ofensivos como vírus e espiões. Por estas razões, antes de conectar um *notebook* na rede LAN, é importante checar se o computador possui antivírus e se este está devidamente atualizado, e checar se não existe nenhum programa espião tentando explorar o ambiente e enviar informações para uma rede externa.

No que se refere ao uso de *notebooks* por funcionários, é importante checar quais acessos estão liberados aos profissionais, pois estes equipamentos proporcionam uma forma simples e discreta para transportar dados da empresa. Estes dados podem ser informações estratégicas cobiçadas pela concorrência. É preciso avaliar se é de interesse da empresa que o funcionário utilize este tipo de equipamento.

Fornecedores e visitantes geralmente solicitam acesso à *internet* para consulta de sites ou e-mails. Nestes casos é interessante possuir uma rede separada, geralmente chamada de *Demilitarized Zone (*DMZ) ou zona desmilitarizada, para conectar estas pessoas diretamente à *internet* sem passar pela rede interna. Desta forma não há necessidade de checar o estado de segurança do equipamento.

Atualmente a Quick Soft possui uma norma de segurança que define que qualquer computador não pertencente ao patrimônio da empresa deve ser apresentado à equipe de suporte antes de ser conectado à rede. O fato de atualmente não existir um método de bloquear estes computadores, permite que por desconhecimento da norma, ou por má conduta, clientes, fornecedores ou funcionários conectem seus computadores à rede sem a devida autorização.

3.2 REQUISITOS PRINCIPAIS DO PROBLEMA A SER TRABALHADO

Abaixo seguem os quadros 1 e 2 com o requisitos funcionais e não funcionais do sistema.

REQUISITOS FUNCIONAIONAS	**CASO DE USO**
RF01. O sistema deverá controlar o acesso ao gerenciamento do sistema através de autenticação por usuário e senha.	UC01
RF02. O sistema deverá permitir ao administrador inserir, alterar, consultar e excluir cadastros de usuários e de equipamentos de rede. O cadastro de equipamentos também poderá ser carregado através de um processo de importação a partir de um arquivo texto.	UC02
RF03. O sistema deverá permitir ao administrador configurar os parâmetros de tempo de histórico de eventos, tempo de sincronização entre o servidor e os clientes de rede, e o envio de e-mails para aviso de eventos de bloqueio.	UC03
RF04. O sistema deverá permitir aos administradores liberar o acesso à rede de um novo equipamento que está sendo bloqueado. Podendo liberar acesso total, ou limitado a determinados equipamentos e por um período determinado.	UC04
RF05. O sistema deverá permitir aos usuários gerar relatórios de equipamentos protegidos, ou seja, dos computadores que possuem o cliente do sistema instalado e de ocorrências de bloqueio de acesso.	UC05

RF06. O sistema deverá ativar as regras criadas pelo administrador nas estações protegidas.	UC06
RF07. O sistema deverá gerenciar possíveis trocas de endereço IP ocasionadas pelo *Dynamic Host Configuration Protocol (DHCP*).	UC07
RF08. O sistema deverá permitir aos administradores cadastrarem regras de bloqueio para os *firewalls*.	UC08

Quadro 1: Requisitos funcionais

REQUISITOS NÃO FUNCIONAIS
RNF01. A interface do console deve ser gráfica, de acordo com um padrão de interface dirigida a menu.
RNF02. O sistema deverá utilizar banco de dados Oracle
RNF03. A console de gerenciamento deverá ser compatível com o sistema operacional Windows versão XP ou superior.
RNF04. A aplicação cliente deverá ser compatível com o sistema operacional Windows versões XP ou superior.

Quadro 2: Requisitos não funcionais

3.3 ESPECIFICAÇÃO

Abaixo segue a especificação do sistema utilizando a *Unified Modeling Language* (UML), demonstrando os casos de uso, de classe e de atividades. A ferramenta escolhida para este processo foi o Enterprise Architect da Sparks.

3.3.1 Diagrama de casos de uso

Na figura 4 é demonstrado o diagrama de casos de uso do software, sendo demonstradas as atividades das duas aplicações do sistema de controle do *firewall* das estações. A aplicação que interage diretamente com o firewall dos computadores protegidos é denominada cliente, e a aplicação central que gerencia os clientes são chamadas de servidor.

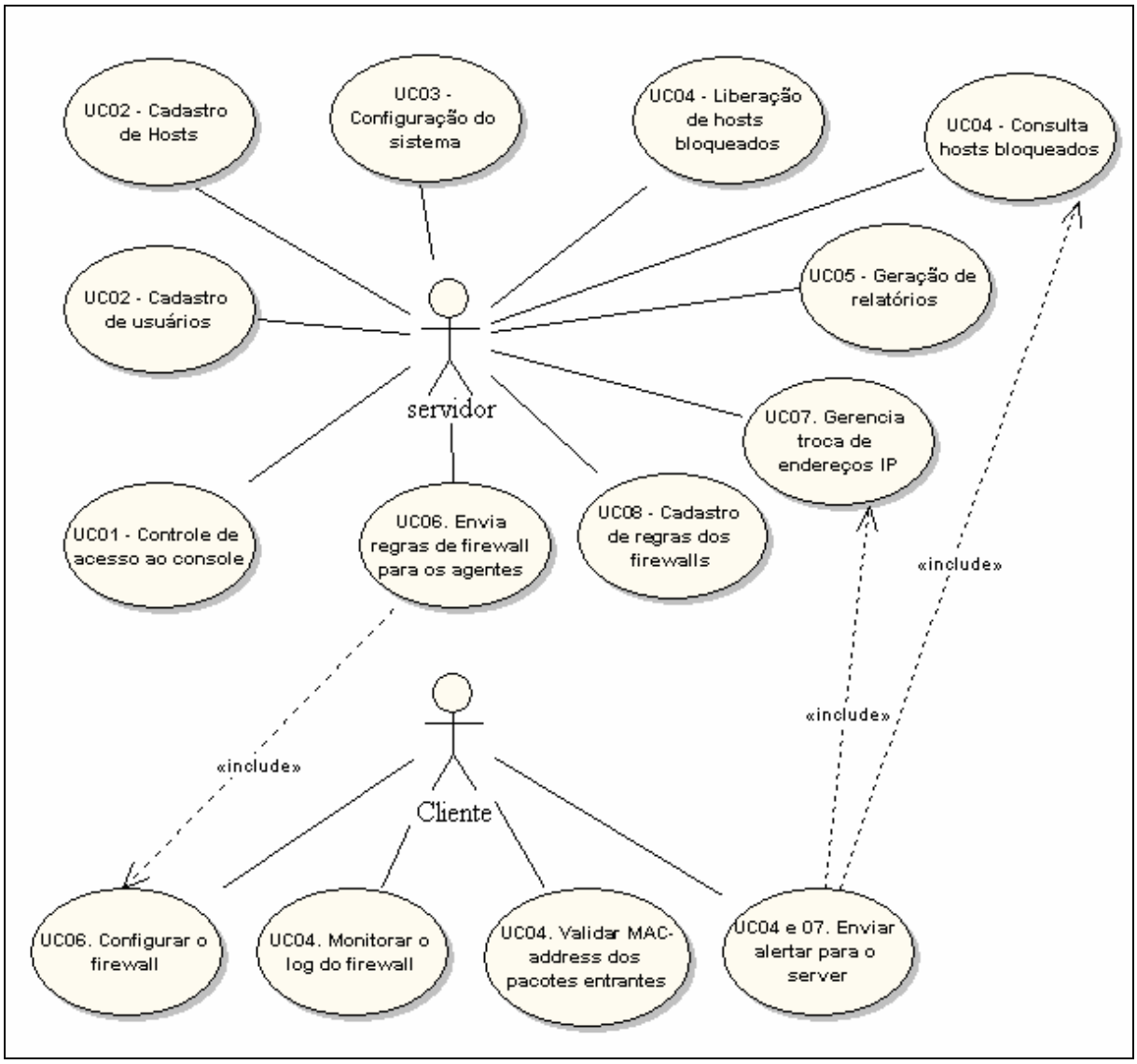


Figura 4: Diagrama de caso de uso conforme requisitos funcionais

Abaixo seguem o detalhamento de cada caso de uso encontrado na figura 4:

a) UC01 - controle de acesso ao console: solicita um usuário e senha para acesso ao console do servidor;

b) UC02 - cadastro de usuários: cadastramento de usuários para administração ou consulta no servidor;

c) UC02 - cadastro de hosts: cadastramento de forma manual ou automática dos computadores protegidos da rede;

d) UC03 - configuração do sistema: configuração dos principais parâmetros do sistema como tempo de retenção dos logs e tempo de sincronismo dos *firewall*;

e) UC04 - consulta dos hosts bloqueados: possibilita aos administradores consultar todos os computadores que foram bloqueados na rede;

f) UC04 - liberação dos hosts bloqueados: possibilita aos administradores liberar os computadores que foram bloqueados na rede, limitando o tempo da liberação e os acessos;

g) UC04 – monitorar o log do *firewall*: o cliente irá monitorar os logs gerados pelo *firewall* do Windows XP, e enviará alertas ao servidor caso ocorram bloqueios;

h) UC04 – validar MAC-addresses dos pacotes entrantes: o cliente irá validar cada pacote recebido no computador protegido, com o objetivo de certificar que o IP origem possui um MAC-address liberado pelo sistema;

i) UC05 - geração de relatórios: possibilita gerar relatórios dos bloqueios e computadores protegidos;

j) UC06 - envia regras de *firewalls* para o cliente: envia as regras cadastradas pelo administrador aos computadores correspondentes;

k) UC06 – configurar o *firewall*: o cliente configura o *firewall* do computador protegido com as regras enviadas pelo servidor;

l) UC07 - gerenciar troca de endereços IP: recebe o alerta do cliente indicando que um computador protegido trocou seu IP. Isto é necessário, pois o *firewall* do Windows XP aceita apenas regras por IP;

m) UC07 – enviar alerta para o servidor: o cliente envia alerta de bloqueios, do estado do firewall (ativado/desativado) e de troca de endereços IP;

n) UC08 - cadastro de regras dos *firewalls*: permite aos administradores cadastrarem regras que serão distribuídas entre os computadores protegidos.

3.3.2 Diagrama de classes

O diagrama de classes demonstra a estruturação das classes utilizadas na especificação da aplicação cliente. Na figura 5 encontram-se as classes do cliente e seus relacionamentos.

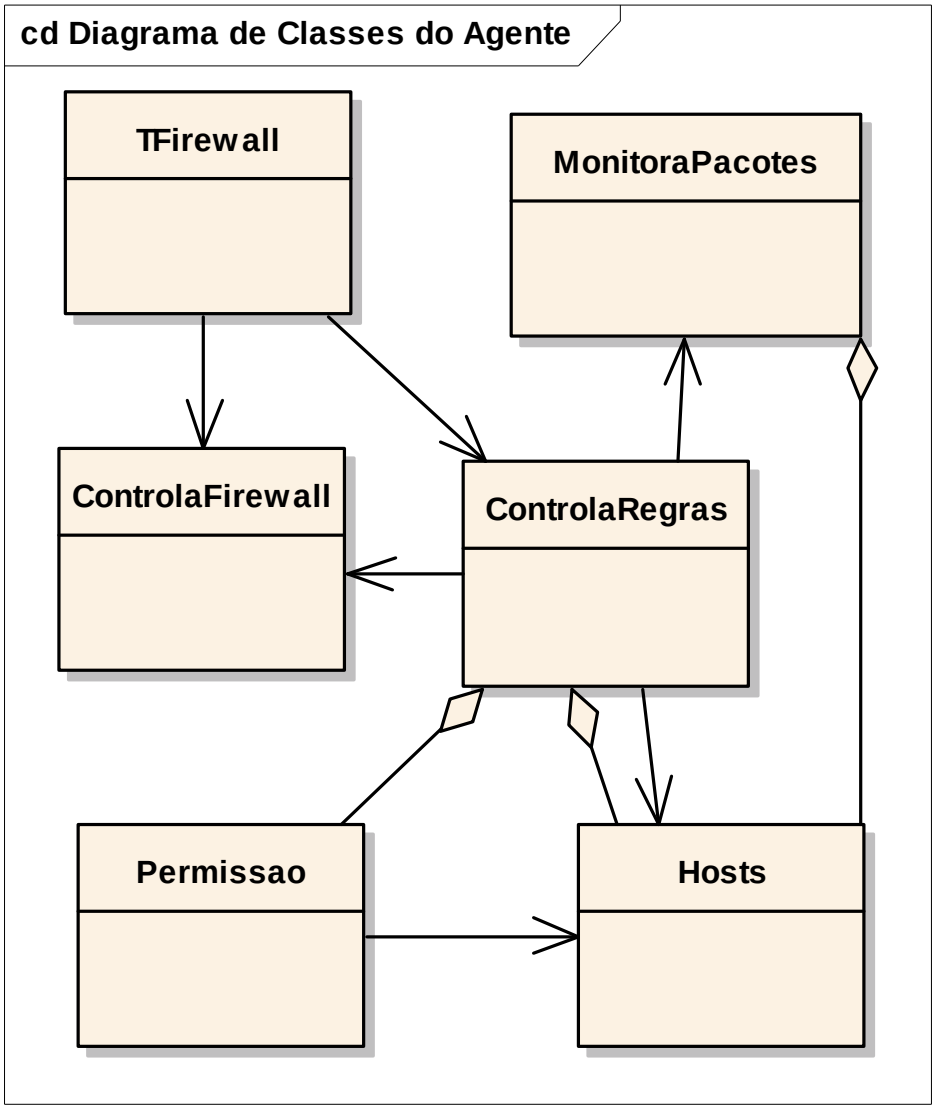


Figura 5: Diagrama de classes do cliente

Figura 6: Detalhamento da classe TFirewall

A classe TFirewall herda da classe TService permitindo que o aplicativo execute em modo *background* no serviço do Windows. Esta classe é responsável também pela comunicação via *socket* com o servidor, recebendo parâmetros e validando informações de inicialização.

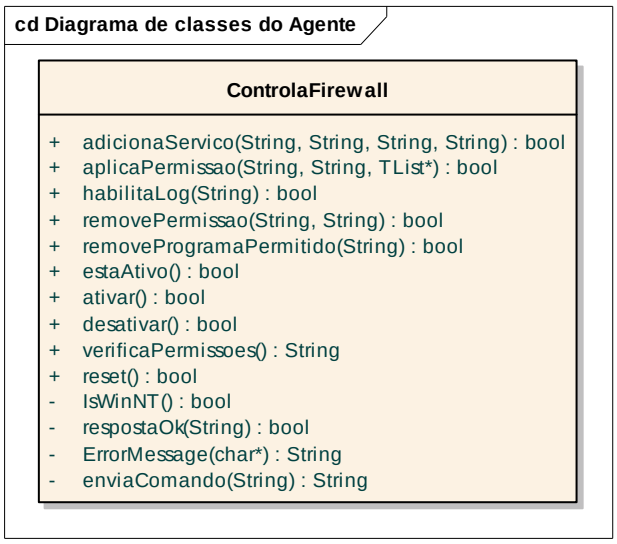


Figura 7: Detalhamento da classe ControlaFirewall

A classe ControlaFirewall é responsável diretamente pela manutenção do *firewall* do computador. Através desta classe são realizados os procedimentos de adição e remoção de regras e verificação do estado do *firewall*.

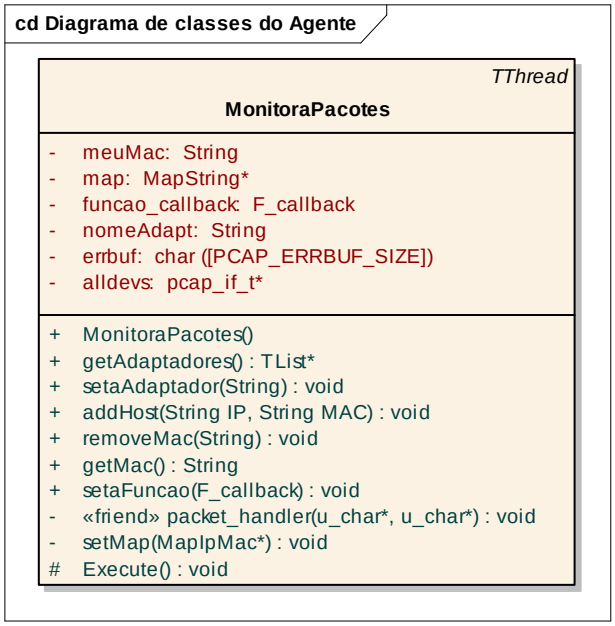


Figura 8: Detalhamento da classe MonitoraPacotes

A Classe MonitoraPacotes é responsável pela configuração do Winpcap que irá monitorar em tempo integral os pacotes entrantes. Sua principal função é validar a relação de endereços IP e MAC dos pacotes recebidos.

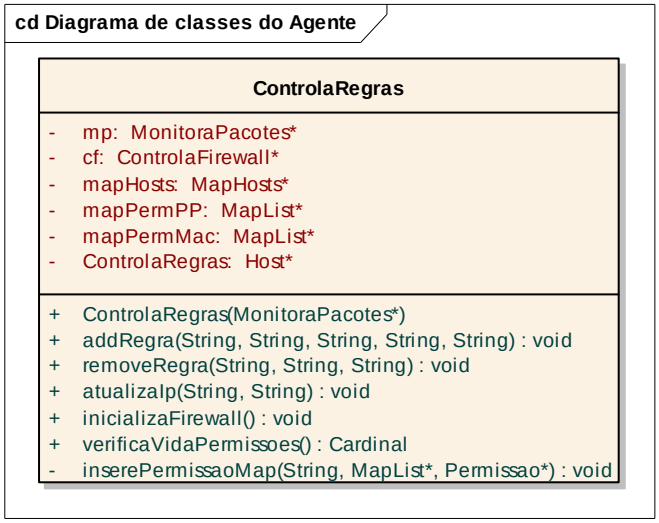


Figura 9: Detalhamento da classe ControlaRegras

A classe ControlaRegras é responsável por montar as regras baseadas em informações de *Hosts* e permissões e encaminhá-las para as classes ControlaFirewall e MonitoraPacotes.

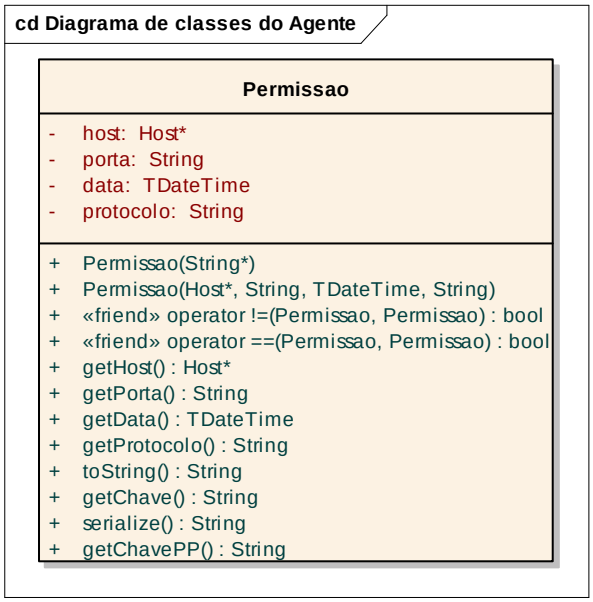


Figura 10: Detalhamento da classe Permissão

A classe Permissao contém as informações de filtros de pacote enviadas pelo servidor como *Host*, porta, protocolo e data para expiração das regras.

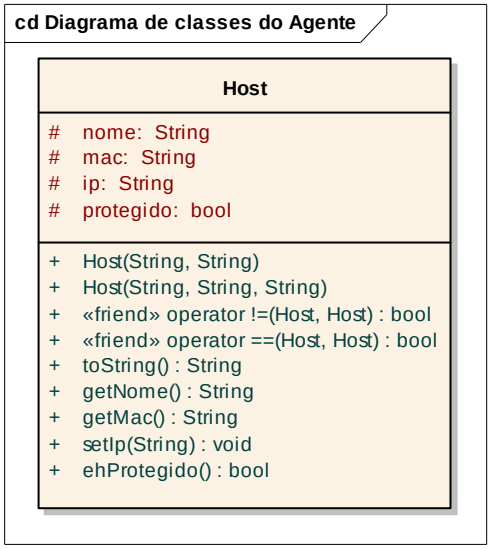


Figura 11: Detalhamento da classe Host

A classe Host é instanciada contendo as informações de endereço IP e MAC dos computadores que possuem acesso a determinado computador protegido.

Na figura 12 estão relacionadas as classes usadas pela aplicação servidor.

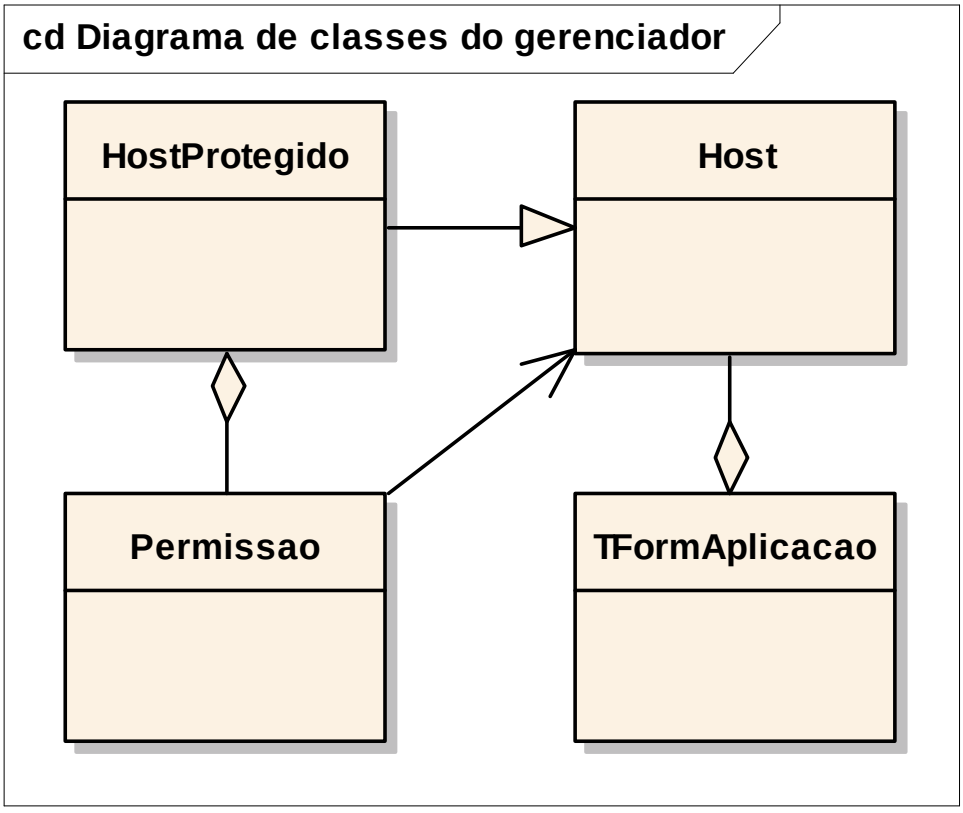


Figura 12: Diagrama de classe servidor

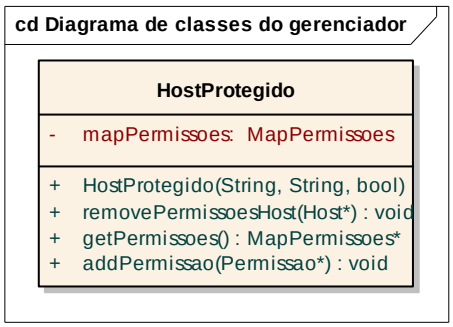


Figura 13: Detalhamento da classe HostProtegido

A classe HostProtegido carrega a lista de permissões de cada computador. Através desta lista é possível saber quais acessos estão liberados para cada computador cadastrado no sistema.

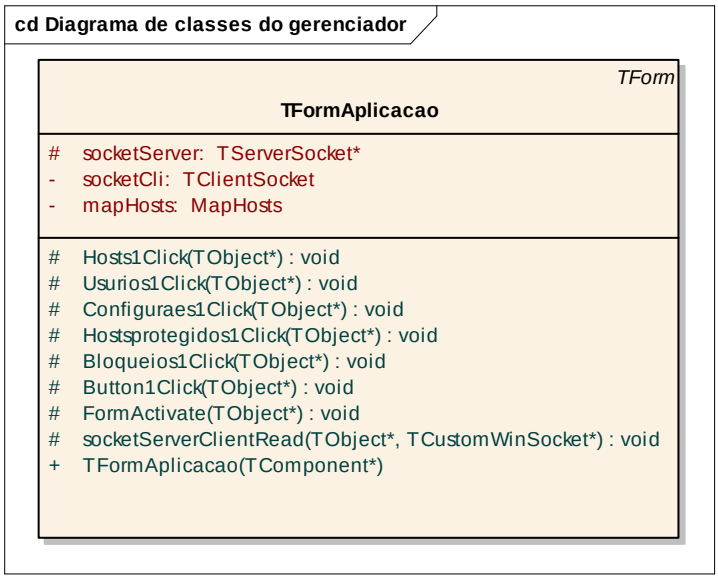


Figura 14: Detalhamento da classe TFormAplicacao

A classe TFormAplicacao é a principal classe do servidor, possuindo uma lista de todos os *Hosts* cadastrados no sistema e demais objetos para o controle da comunicação com os clientes através de *sockets*.

As classes Permissão e Host da aplicação servidor possuem as mesmas funcionalidades das classes Permissão e Host da aplicação cliente.

3.3.3 Diagrama de atividades

O diagrama de atividades apresentado na figura 15 demonstra a interação da aplicação cliente com o *firewall* do Windows XP e com a aplicação servidor. A ativação do cliente é feita pelos serviços do Windows, e o tempo de sincronismo é parametrizado no servidor pelo administrador da rede.

No diagrama da figura 16 são demonstradas as principais comunicações entre o cliente e o servidor. O servidor envia atualizações aos clientes resultantes de alterações ou criação de regras.

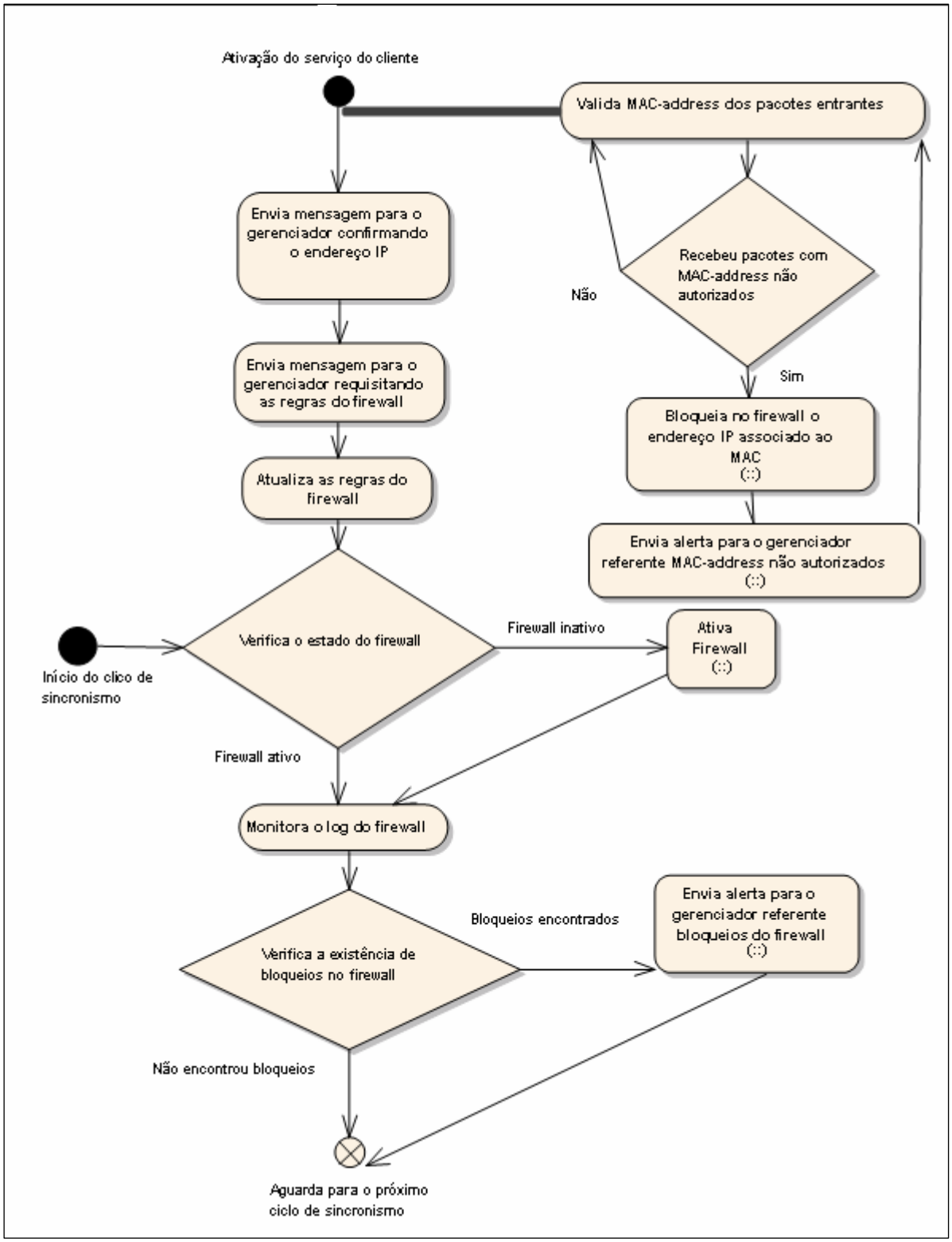


Figura 15: Diagrama de atividades do cliente

Na figura 15 são demonstradas as principais atividades da aplicação cliente, que ao ser ativada pelo serviço do Windows, realiza as ações de confirmação do endereço IP do computador protegido, solicitação e atualização de regras de *firewall*.

Após a ativação das regras de firewall, a aplicação cliente entra em ciclo onde é checado se o firewall está ativo e se há bloqueios registrados em seus logs. Havendo bloqueios, será enviado alerta aos administradores da rede.

Em paralelo as atividade acima citadas, é ativado o processo que irá validar o endereço MAC dos pacotes recebidos no computador para complementar a proteção exercida pelo *firewall*. Caso o processo de validação de endereços MAC detecte um pacote originado de um endereço IP liberado no firewall com seu endereço MAC autorizado, será automaticamente removida as regras que liberam este determinado endereço IP.

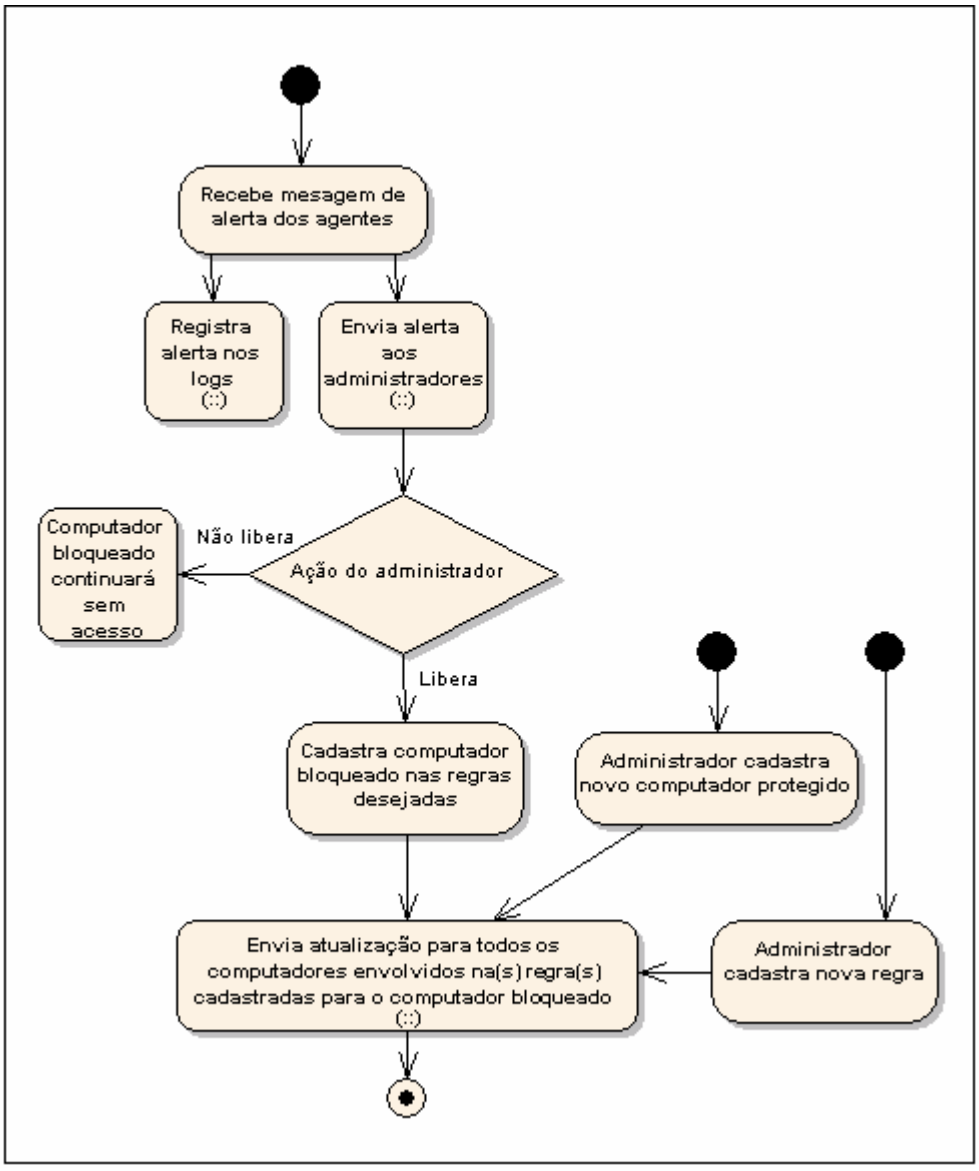


Figura 16: Diagrama de atividades do servidor

Na figura 16 são demonstradas as atividades da aplicação servidor que ao receber mensagens de alerta das aplicações cliente, registra no banco de dados as informações, gera alerta na interface de gerenciamento e se estiver parametrizado irá enviar e-mails aos administradores da rede.

Os administradores da rede podem cadastrar o computador bloqueado no sistema para que se possa criar regras de liberação de acesso. Ao criar regras de *firewall*, o servidor irá disparar automaticamente atualizações a todos os computadores envolvidos com aquela determinada regra recém criada.

3.4 IMPLEMENTAÇÃO

A seguir será apresentado o detalhamento da implementação do software, de acordo com as especificações apresentadas neste documento.

3.4.1 Técnicas e ferramentas utilizadas

Para implementação do cliente e do servidor do sistema, foi utilizada a linguagem C++ Builder Enterprise Suite versão 6.0 da Borland. No cliente foi utilizada a biblioteca Winpcap para capturar os pacotes da rede com o objetivo de validar o endereço MAC origem.

O WinPcap é uma ferramenta para monitoração da rede em ambientes Microsoft Windows, permitindo as aplicações capturar pacotes da rede. Através do Winpcap é possível criar filtros e capturar somente informações desejadas, como todos os pacotes enviados para uma determinada placa de rede (WINPCAP, 2006).

Nas figuras 16 e 17 são demonstrados trechos do código da classe MonitoraPacotes utilizando o Winpcap através do método Execute.

```
if ((adhandle= pcap_open_live(d->name,     // name of the device
   65536,                  // portion of the packet to capture.
 // 65536 grants that the whole packet will be captured on all the MACs.
    1,                     // promiscuous mode (nonzero means promiscuous)
       1000,                        // read timeout
      errbuf                        // error buffer
                                     )) == NULL)
{
      String erro = "Impossivel abrir adaptador. ";
      erro+= d->name;
      erro+= "não é suportado pelo WinpCap";
}
```

Figura 17: Código utilizando a biblioteca do Winpcap para abrir a placa de rede

```
   char filtro[28]="";
   sprintf(filtro, "ether dst %s", (getMac()).c_str());

   //compila o filto
   if(pcap_compile(adhandle, &fcode, filtro, 1, netmask) <0 ){
      pcap_freealldevs(alldevs);
      throw new MonitoraPacotesException("Erro ao compilar filtro");
   }
   //seta o filtro no adaptador
   if(pcap_setfilter(adhandle, &fcode)<0){
      pcap_freealldevs(alldevs);
      throw new MonitoraPacotesException("Erro ao setar o filtro");
   }
```

Figura 18: Código para definir um filtro de pacotes via Winpcap

Conforme descrito neste documento, foi utilizado o sistema de *firewall* do Microsoft Windows XP SP2 para a proteção de cada computador da rede LAN. O sistema de *firewall* do Windows permite seu gerenciamento através de linha de comando conforme exemplo demonstrado na figura 19.

```
netsh firewall reset
(remove as configurações adicionais que possam existir)

netsh firewall delete allowedprogram C:\WINDOWS\system32\sessmgr.exe
(remove o acesso via assistência remota para qualquer IP conforme configuração padrão)

netsh firewall set logging filelocation = C:\WINDOWS\pfirewall.log maxfilesize = 4096
droppedpackets = enable
(Ativa o sistema de log do firewall para registrar apenas os pacotes bloqueados)

netsh firewall add portopening TCP 5900  VNC enable custom 192.168.0.1, 192.168.0.2,
192.168.0.3
(implementa regras cadastrada no sistema)

netsh firewall set opmode enable
(ativa o firewall)
```

Figura 19: Linha de comando para gerenciamento do firewall do Microsoft Windows XP SP2.

O cliente utiliza a classe ControlaFirewall para ativar, adicionar e remover regras e monitorar o log do *firewall* através da linha de comando conforme descrito na figura 19. Na figura 20 segue o código da classe ControlaFirewall executando o método enviaComando.

```
GetStartupInfo(&si);      //set startupinfo for the spawned process

si.dwFlags = STARTF_USESTDHANDLES|STARTF_USESHOWWINDOW;
si.wShowWindow = SW_HIDE;
si.hStdOutput = newstdout;
si.hStdError = newstdout;     //set the new handles for the child process
si.hStdInput = newstdin;

//spawn the child process
if (!CreateProcess(NETSH,NULL,NULL,NULL,TRUE,CREATE_NEW_CONSOLE,
            NULL,NULL,&si,&pi))
{
  return ErrorMessage("CreateProcess");
}
```

Figura 20: Código para inicializar o envio de comandos ao *firewall*

3.4.2 Operacionalidade da implementação

Conforme descrito no diagrama de caso de uso, o sistema Controle de Acesso de Notebooks, Desktops e Ativos de uma rede LAN é dividido em duas partes: servidor e cliente.

O servidor possui a interface com o administrador, onde é possível o cadastro de usuários para administração do sistema, regras para os *firewalls* internos, computadores protegidos e parametrização do ambiente. O servidor envia atualizações para os clientes quando ocorrem alterações no cadastro de regras ou alterações no cadastro de computadores.

Abaixo seguem as principais telas de servidor

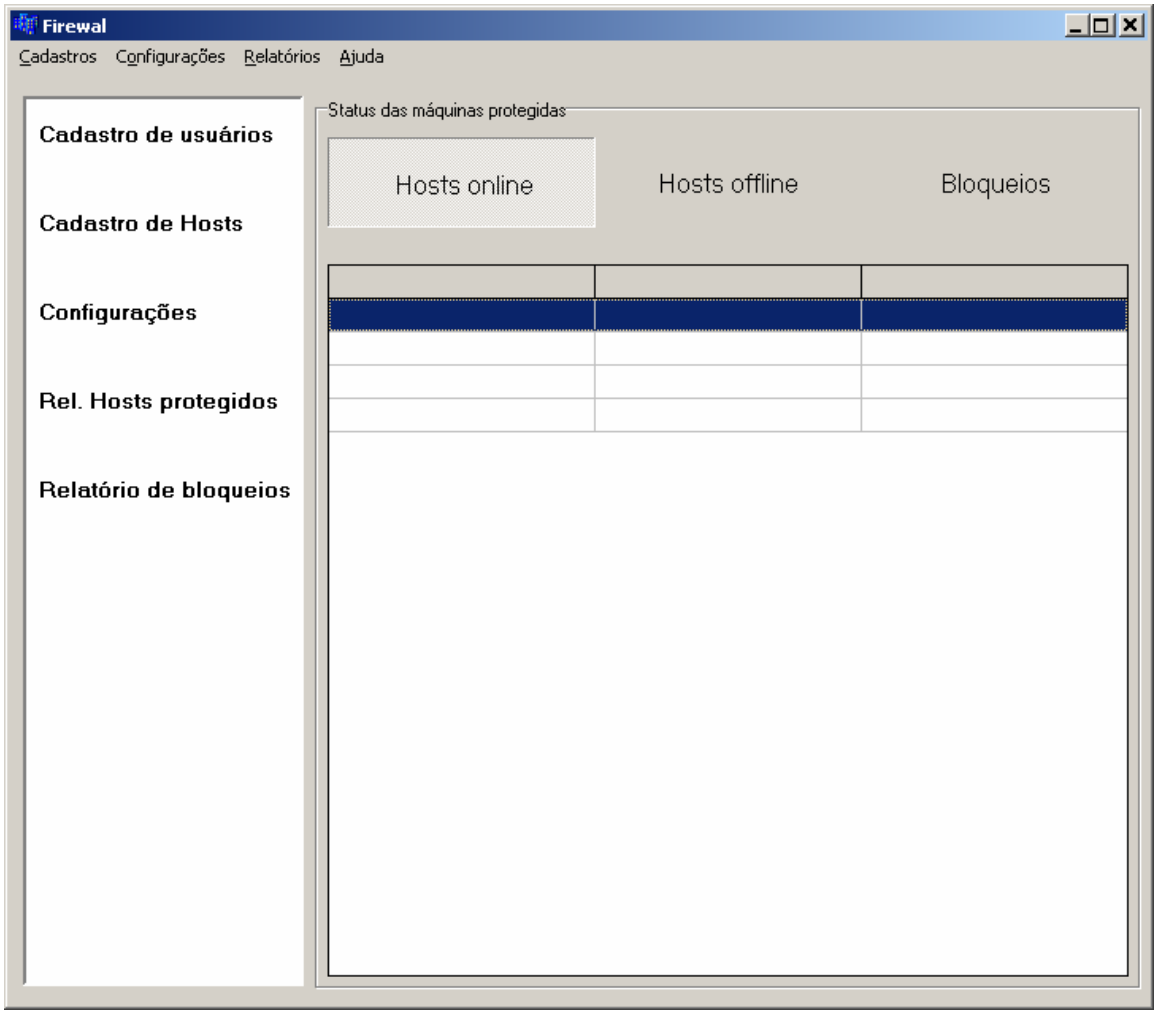


Figura 21: Tela principal do servidor

Na Tela principal do sistema são encontrados os menus de cadastro, configurações, relatórios e a console os *Hosts* que estão ativos, desativados e bloqueados.

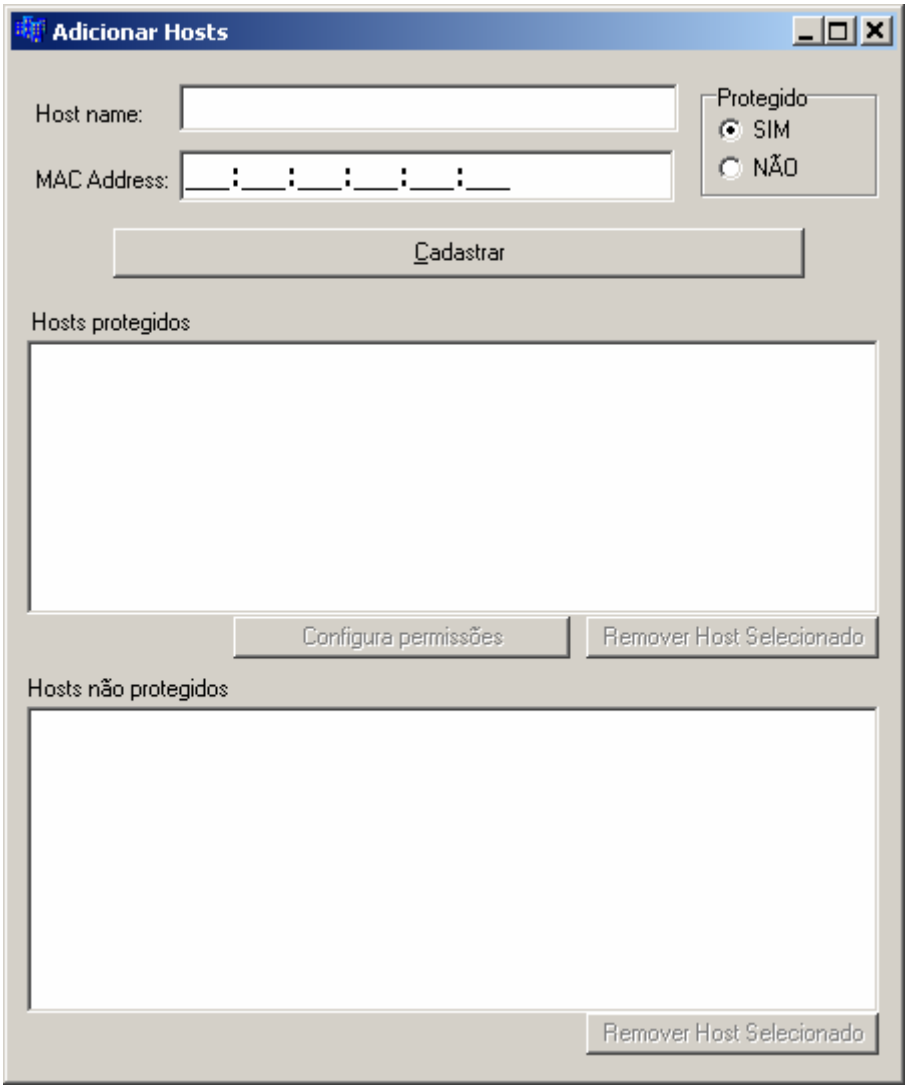


Figura 22: Tela de cadastro de *Hosts*

Na tela de cadastro dos *Hosts* é possível cadastrar os computadores com seus devidos endereços MAC, indicar se eles são protegidos ou não e associa-los a regras de *firewall*.

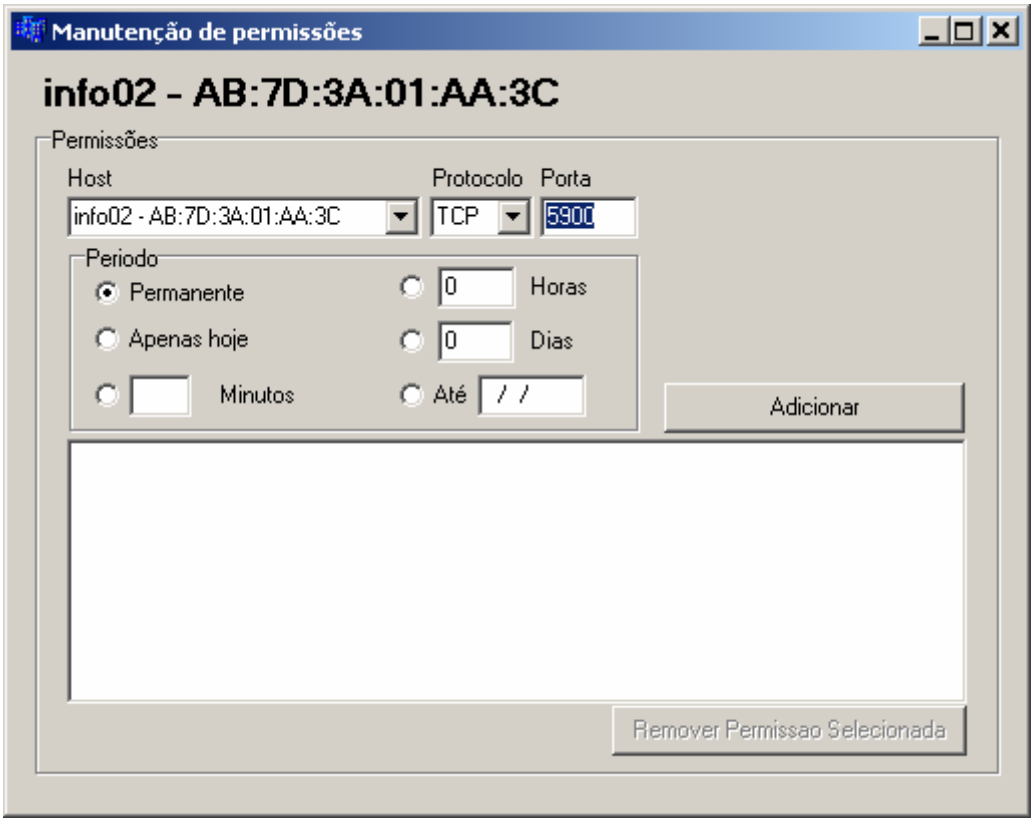


Figura 23: Tela de manutenção de permissões

Na tela de manutenção de permissões é possível ao administrador criar regras para o computador que está sendo cadastrado. Esta regra pode ser permanente ou temporária, podendo ser configurada por minutos, horas e dias.

O cliente é instalado em todos os computadores com o sistema operacional Windows versão XP SP2 ou maior cujo administradores da rede desejam proteger. O cliente não possui interface com o usuário sendo iniciado pelo serviço do Windows, e executa basicamente as funções de configuração e monitoração do *firewall*.

Todas as regras de *firewall* cadastradas através do gerenciado são baseadas em endereços IP, pois o *firewall* do Windows não possui funções de filtro de pacotes pelo *MAC-adress*. Para evitar que computadores não autorizados burlem as regras utilizando endereços IP cadastrados, é utilizado a biblioteca *Winpcap* para validar os *MAC-address* entrantes. Quando é detectado um *MAC-address* não autorizado com endereço IP liberado no *firewall*, o cliente irá redefinir as regras do *firewall* bloqueando este endereço IP e irá enviar um alerta ao

servidor..

Na figura 24 é demonstrado um macro esquema da solução de segurança do sistema:

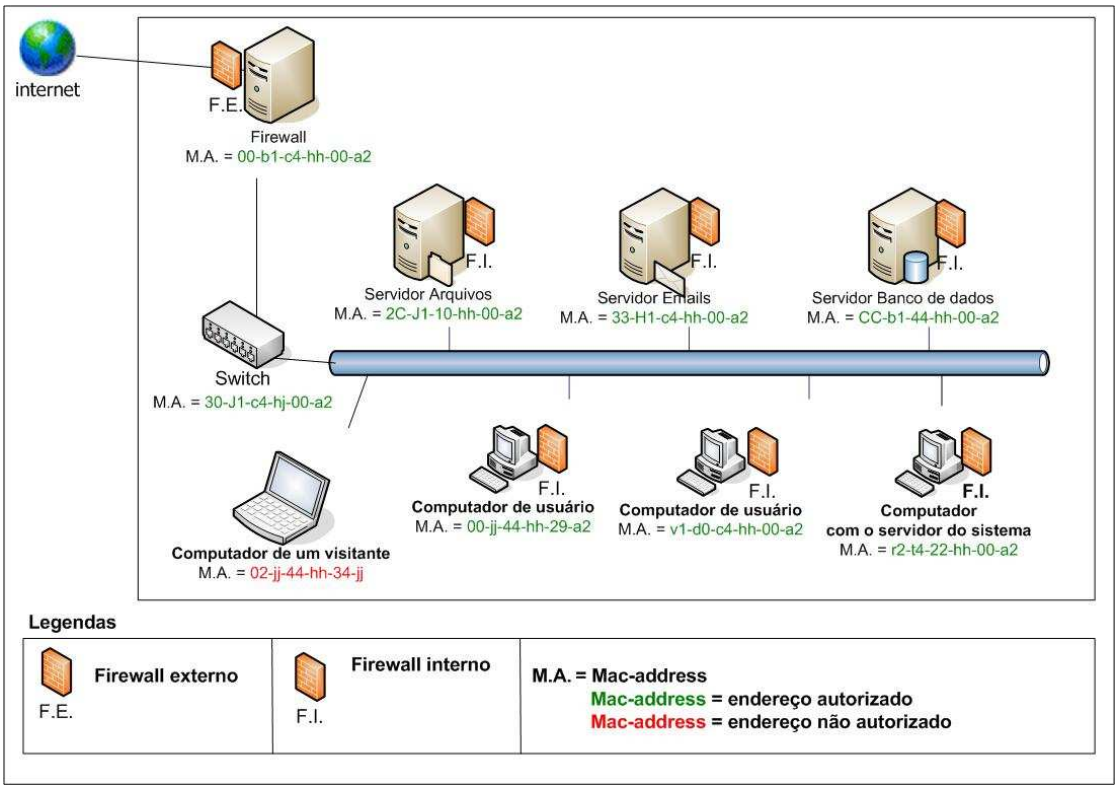


Figura 24: Exemplo de uma rede LAN protegida pelo sistema

Com base na figura 24, pode ser exemplificado o seguinte estudo de caso.

Em um ambiente protegido pelo sistema de controle de acesso, um visitante da empresa provido de um notebook tentará acessar a rede sem solicitar a devida autorização. Ao conectar seu notebook na rede, ele receberá normalmente o endereço IP do servidor de DHCP, porém ao tentar acessar qualquer um dos computadores protegidos será bloqueado pelo firewall interno.

A aplicação cliente instalada nos computadores protegidos irá gerar alerta para os administradores da rede, para que estes possam tomar as devidas providências. Caso seja realmente necessário liberar o acesso para o visitante, os administradores poderão criar regrar temporárias que permitirão determinados acessos por um tempo limitado.

3.5 RESULTADOS E DISCUSSÃO

Durante os testes em laboratório, o cliente do sistema mostrou-se eficiente no processo de interação com o *firewall* do Windows XP SP2. Foram realizados testes de manutenção de regras de *firewall*, monitoração de logs e validação da operacionalidade dos serviços.

Nos testes do servidor do sistema foram acompanhadas as ações do servidor após a recepção de alertas de bloqueios e alterações de endereço IP. Nas funções de cadastramentos, navegação de telas, consultas e relatórios, foi testada a simplicidade de utilização.

Os principais testes realizados e seus resultados são demonstrados no quadro 3:

Descrição do teste	**Resultado obtido**
Usuário desativou o *firewall* do Windows	No tempo do ciclo de sincronismo parametrizado pelo sistema, o cliente detectou a falha, corrigiu e gerou um alerta para os administradores da rede.
Usuário desativou o serviço do cliente	No tempo do ciclo de sincronismo parametrizado pelo sistema, o servidor detectou a falha gerando um alerta para os administradores da rede.
O firewall bloqueou pacotes de um computador não autorizado	O cliente enviou alerta para os administradores da rede, para que seja tomado alguma ação.
O cliente detectou um endereço de MAC não autorizado enviando pacotes com sucesso para o computador protegido	O cliente automaticamente criou uma regra para bloqueio do endereço IP associado ao MAC não autorizado.
Os administradores da rede criaram e alteraram regras para os *firewalls*	O servidor realizou o processo de atualização nos computadores relacionados com as regras criadas e alteradas.
Simulado a troca de endereço IP do computador do usuário pelo sistema de DHCP	O cliente enviou para o servidor o novo endereço do computador. O servidor ajustou as regras associadas ao MAC deste computador e atualizou os *firewalls* de todas as estações envolvidas.

Quadro 3: Resultado dos testes em laboratório

Uma vantagem importante observada neste sistema em comparação ao seu correlato chamado Strongman (KEROMYTIS, 2001), é que no momento de liberar acesso a um computador visitante, é preciso configurar o computador do visitante com as chaves necessárias para acesso a cada serviços desejado. Além do esforço extra, há o risco do sistema operacional utilizado pelo visitante não ser compatível com a segurança adotada. Outro problema é limitar o tempo de liberação deste visitante, nada impedirá que este computador

acesse a rede em outro momento não autorizado usando as mesmas chaves.

4 CONCLUSÕES

A realização deste trabalho demonstrou a possibilidade de proteger os computadores de uma rede LAN de possíveis invasores internos através de *firewalls* distribuídos de uma forma simples e eficiente. Observou-se o controle de acesso pelo endereço MAC, gerenciado através de um console central dos administradores da rede.

Outra vantagem deste sistema é o desenho das classes que foram projetadas de modo a facilitar a portabilidade para outros sistemas de *firewall* que possuam gerenciamento por linha de comando.

O sistema de *firewall* do Microsoft Windows XP SP2 possui inúmeras limitações se comparado com o IPTABLES que é a ferramenta de *firewall* mais comum encontrada em servidores Linux, porém seus filtros básicos aliados às funcionalidades do cliente do sistema foram suficientes para cumprir com os requisitos mencionados neste documento.

Uma possível limitação prevista neste sistema é a impossibilidade de controle de acesso via endereços MAC em uma rede WAN. Ao passar por um roteador, o pacote de rede terá seu endereço de MAC origem alterado para o endereço do roteador, fazendo com que todos os pacotes originados por uma rede tenham o mesmo endereço MAC. Estuda-se para um trabalho futuro a solução de colocar um gerenciador de *firewalls* distribuídos em cada rede de uma WAN.

4.1 EXTENSÕES

Como sugestão para extensão deste trabalho, sugere-se a adaptação de um sistema *firewall* de código aberto, que possa ser utilizado também nas plataformas Microsoft Windows 98 e 2000 devido a muitas empresas ainda utilizarem estas versões.

REFERÊNCIAS BIBLIOGRÁFICAS

COMER, Douglas E. **Interligação em rede com TCP/IP**. Tradução de ARX Publicações. Rio de Janeiro: Campus, 1998.

GOMES, Olavo J. A. **Segurança total**. Sao Paulo: Makron Books, 2000. 276p.

KEROMYTIS, Angelos D.***Strongman*:** A Scalable solution to trust management in networks. Disponível em: http://www1.cs.columbia.edu/~angelos/Papers/diss.pdf. Acessado em 5 Nov. 2005.

KUROSE, James F.; ROSS, Keith W. **Computer networking**: a top-down approach featuring the Internet. Boston: Addison Wesley, 2001.

LOPES, Raquel V.; SAUVÉ, Jacques P.; NICOLLETTI, Pedro S. **Melhores práticas para Gerência de Redes de Computadores**. Rio de Janeiro: Campus, 2003.

MICROSOFT [2000]. Disponível em <http://technet.microsoft.com/network/tcp>. Acesso em: 12 Dez. 2005.

RUBIN, Aviel D.; CHESWICK, William R.**White-hat security arsenal**: tackling the threats. Boston: Addison-Wesley, 2001.

RUBIN, Aviel D.; CHESWICK, William R.; BELLOVIN, Steven M. **Firewalls e segurança na internet**: repelindo o hacker ardiloso. Tradução Edson Furmankiewicz. - 2. ed. - Porto Alegre: Bookman, 2005.

SOARES, Luis F. G.; LEMOS, Guido; COLCHER, Sergio. Redes de computadores: das LANs MANs e WANs as redes ATM. Rio de Janeiro: Campus, 1995.

TORRES, Gabriel. **Redes de computadores**: curso completo. Rio De Janeiro: Axcel Books, c2001.

WINPCAP [2006]. Disponível em <http://www.winpcap.org>. Acesso em: 10 Mai. 2006.