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

Autor: David Krzizanowski
Orientador: Francisco Adell Péricas

# Roteiro da apresentação

- Introdução
- Objetivos
- Desenvolvimento
- Conclusões
- Extensão

# Introdução

- Por que devemos nos preocupar com o que entra e sai de uma rede de computadores?
  - Vulnerabilidades dos sistemas;
  - Administração inadequada da segurança das informações;
  - Desconhecimento dos perigos por parte dos usuários finais.

- Quais são os principais “vilões” deste cenário?
  - Softwares maliciosos: vírus, *spyware*, *addware*, *trojans*, etc;
  - Pessoas interessadas em espionagem ou sabotagem.

# Introdução

- Por que a segurança deve ser mais rígida para usuários de computadores móveis (notebooks)?
  - Uso doméstico com pouca proteção;
  - Geralmente os sistemas de proteção estão desatualizados ou inexistentes ( antivírus, atualizações automáticas do sistema operacional, firewall );
  - Facilita a entrada e saída de informações da empresa sem o devido controle.

- Como as empresas estão se protegendo?
  - Sistema de *Firewall* para proteger a rede LAN de acessos advindos da internet;

# Introdução

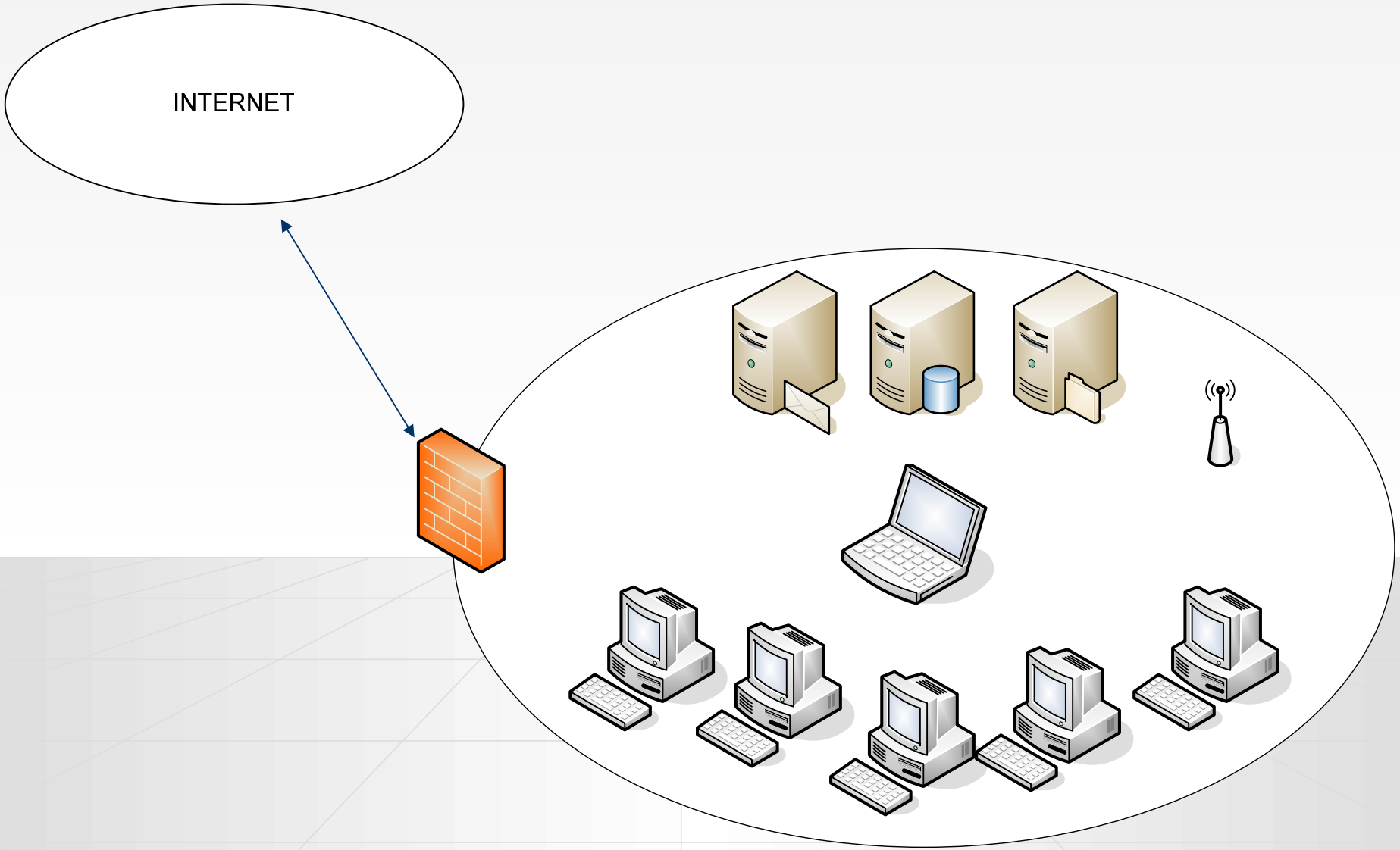
- Sistema de PROXY para controlar os acessos às páginas HTML;
- Regras no servidor de e-mails para impedir a entrada de conteúdos suspeitos;
- Sistema de antivírus no servidor de e-mails e estações para tentar evitar ataques de softwares maliciosos.

- Algumas formas utilizadas por empresas para controle de acesso a rede LAN:
  - Servidor DHCP configurado para distribuir endereços apenas para os endereços MAC cadastrados;

# Introdução

- Utilização de chaves de autenticação privada;
- Switchs gerenciáveis com capacidade de bloquear tráfego de pacotes enviados por endereços MAC não cadastrados.

# Exemplo de um ambiente Corporativo



# Objetivos

- O objetivo do trabalho:
  - Especificação e implementação de um software de controle de acesso as estações e servidores Windows em uma rede LAN através de gerenciamento de firewalls distribuídos;

- Objetivos específicos:
  - Gerenciamento do firewall do Windows XP SP2 ou Server 2003 SP1;
  - Interceptação e interpretação de pacotes TCP/IP para controle de acesso dos equipamentos de rede;

# Objetivos

- Monitoração de atividades de bloqueio dos firewalls;
- Armazenamento de informações monitoradas.

# Desenvolvimento

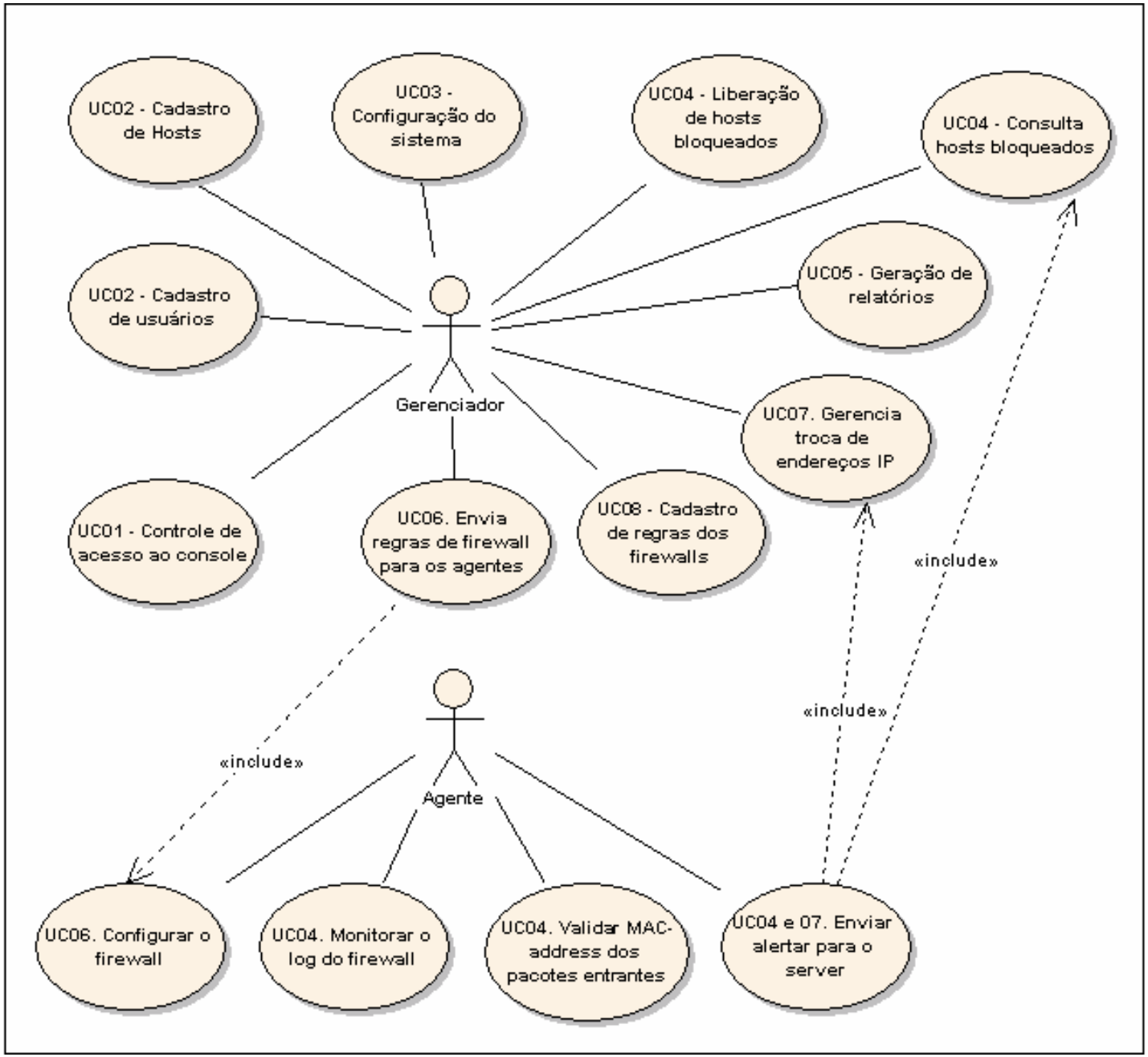
- Requisitos Funcionais:
  - Autenticação para acesso ao gerenciador;
  - Cadastros de usuários e computadores;
  - Parametrização dos tempos de sincronismo entre gerenciador e agentes, de envio de e-mails e de retenção de históricos;
  - Possibilitar liberação personalizada para eventos de bloqueio;
  - Geração de relatórios de equipamentos protegidos e eventos de bloqueios;
  - Criação de regras de firewalls;

# Desenvolvimento

- Requisitos Funcionais:
  - Ativação das regras nos firewalls distribuídos;
  - Validar o endereço MAC nos pacotes recebidos nas estações protegidas.

# Desenvolvimento

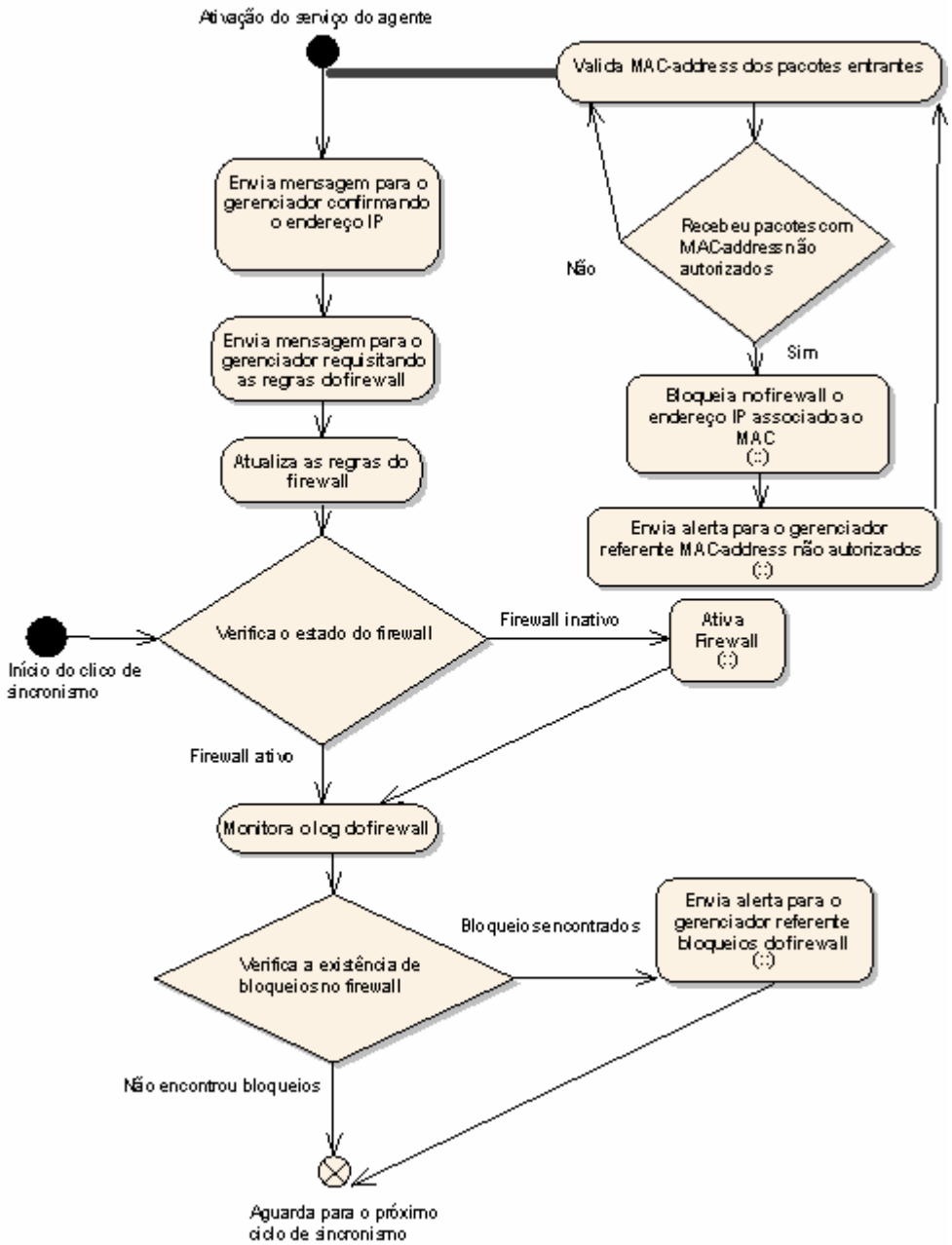
- Especificação:
  - Caso de uso:


UC02 - Cadastro de Hosts
UC03 - Configuração do sistema
UC04 - Liberação de hosts bloqueados
UC04 - Consulta hosts bloqueados
UC02 - Cadastro de usuários
UC05 - Geração de relatórios
Gerenciador
UC07. Gerencia troca de endereços IP
UC01 - Controle de acesso ao console
UC06. Envia regras de firewall para os agentes
UC08 - Cadastro de regras dos firewalls
«include»
«include»
«include»
Agente
UC06. Configurar o firewall
UC04. Monitorar o log do firewall
UC04. Validar MAC-address dos pacotes entrantes
UC04 e 07. Enviar alertar para o server

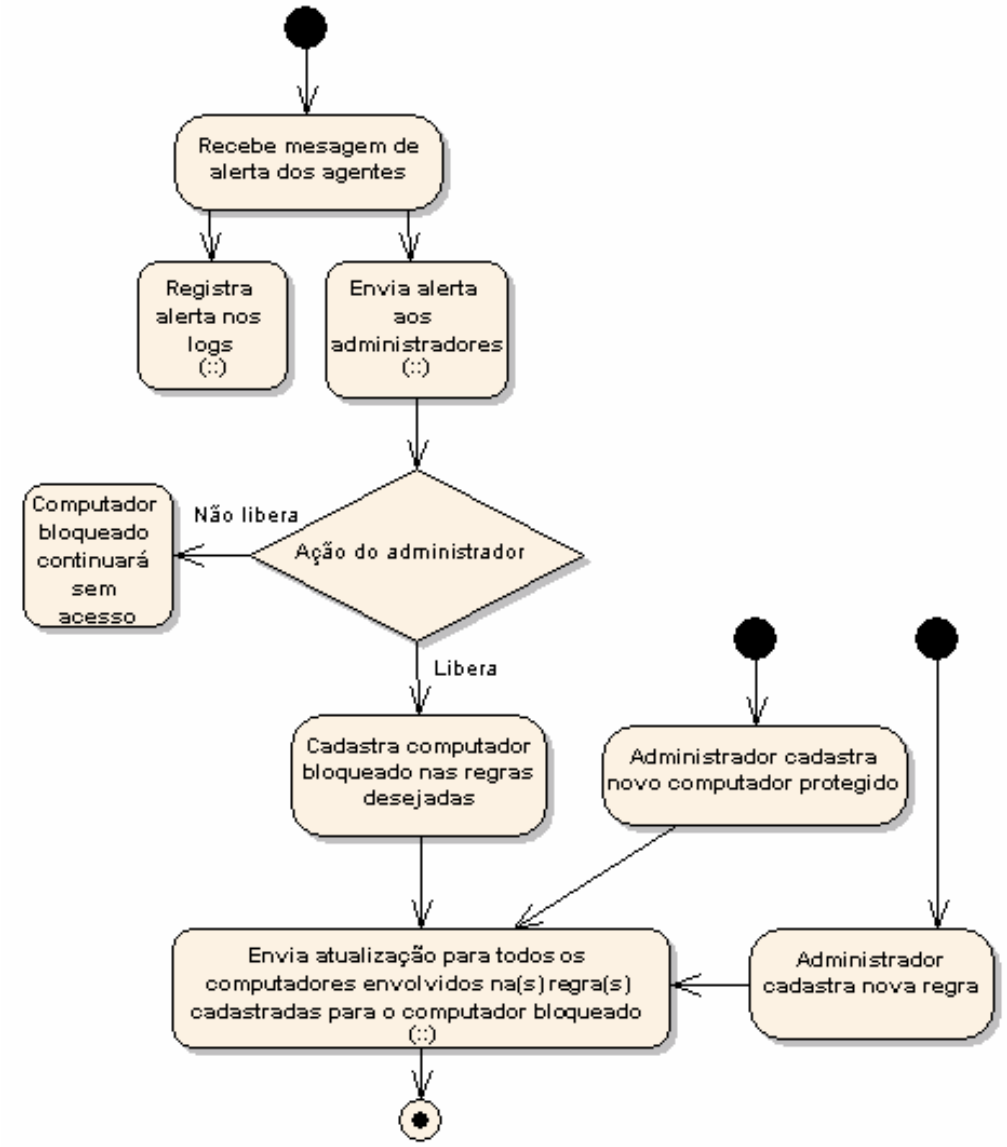
# Desenvolvimento

- Especificação:
  - Caso de uso:
  - Caso de atividades:

# DIAGRAMA DE ATIVIDADES DO AGENTE



# DIAGRAMA DE ATIVIDADES DO GERENCIADOR

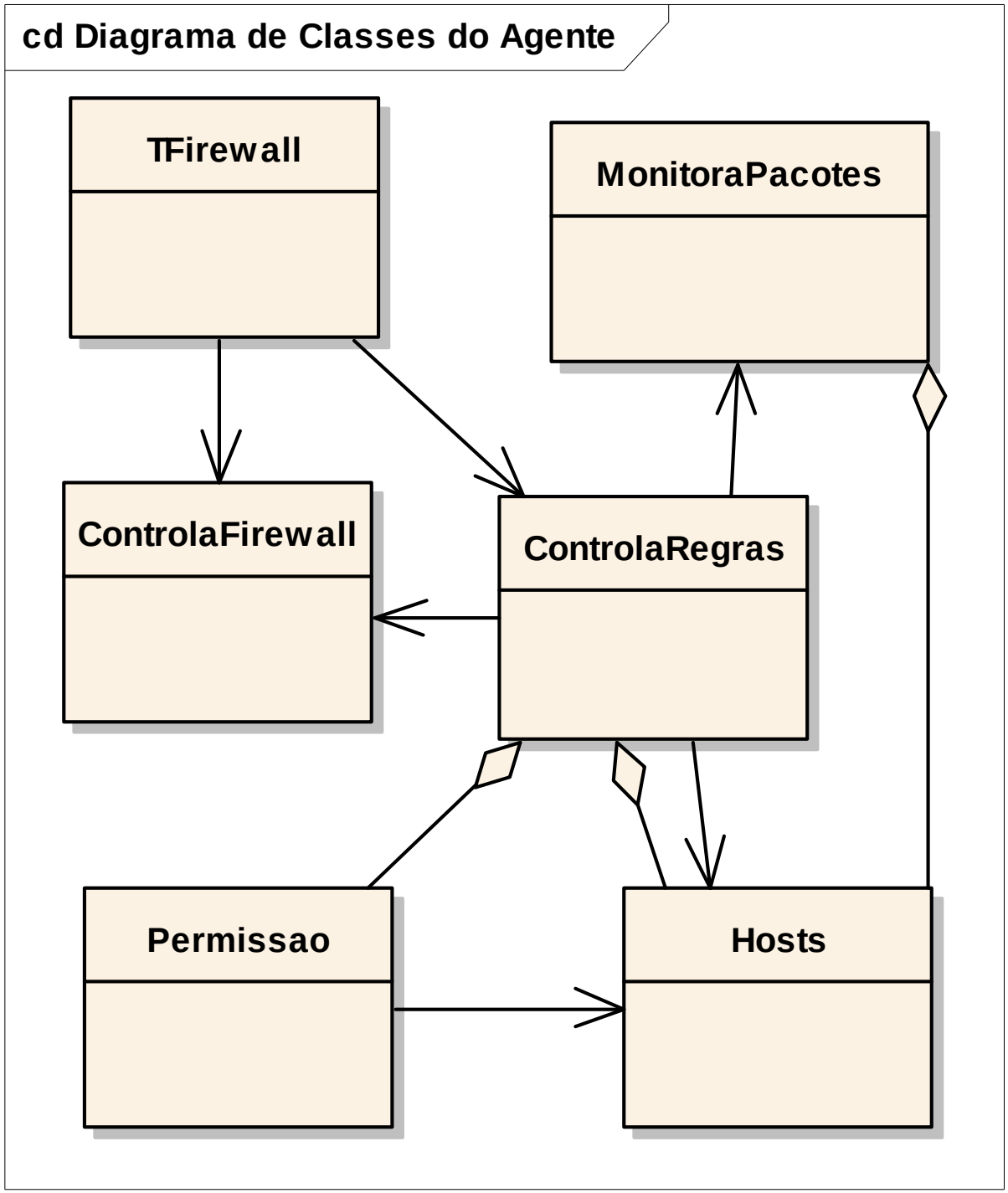


# Desenvolvimento

- Implementação:
  - Ferramenta de desenvolvimento: Borland C++ Builder Enterprise Suite 6.0;
  - Componentes principais:
    - Gerenciador – Timers, database, query e socket;
    - Agente – Winpcap, timers, socket.
  - Área de armazenamento de dados: Oracle Database Express Edition (10g).

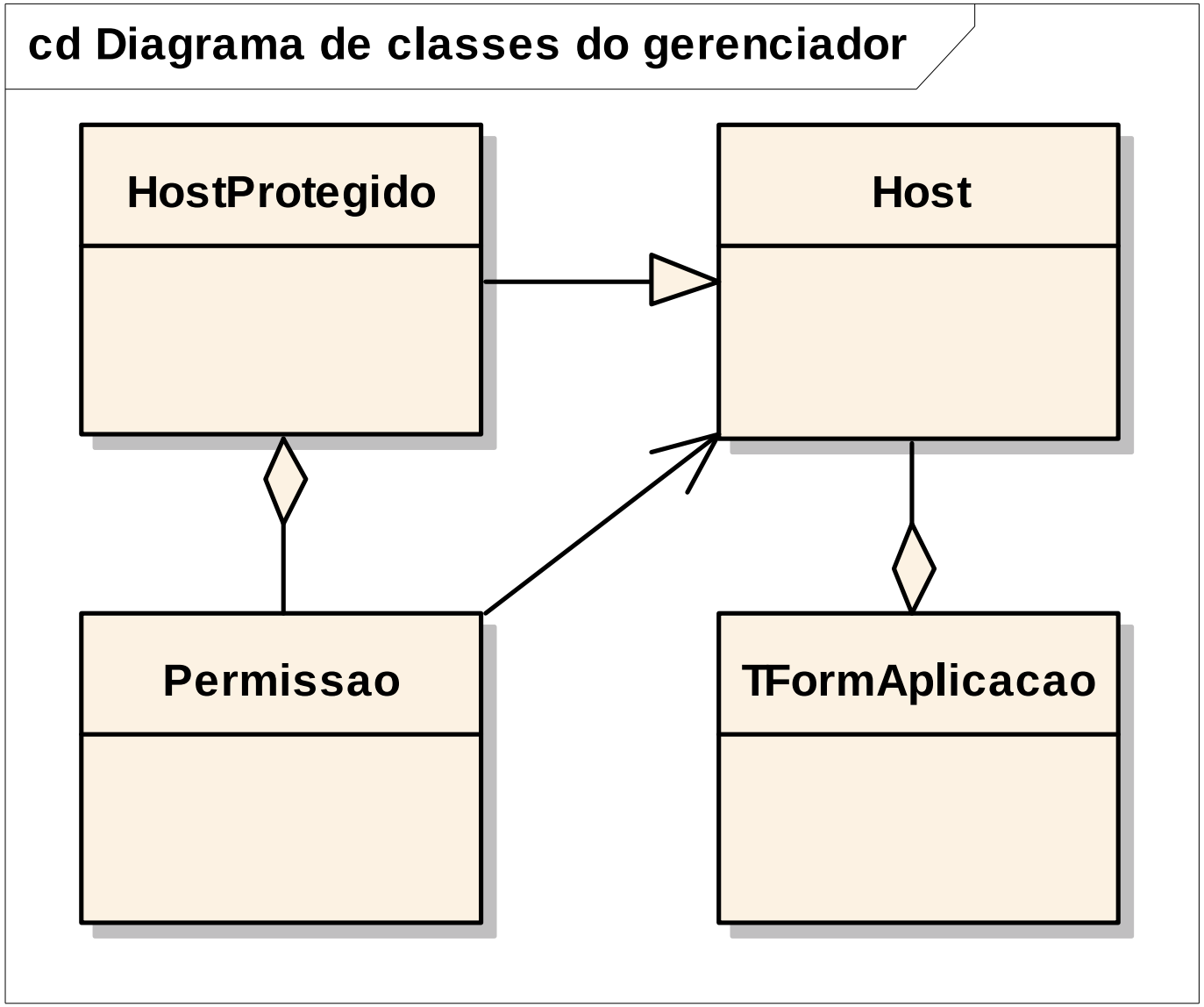
# Desenvolvimento

- Implementação:
  - Diagrama de classes do agente:


cd Diagrama de Classes do Agente
TFirewall
MonitoraPacotes
ControlaFirewall
ControlaRegras
Permissao
Hosts

# Desenvolvimento

- Implementação:
  - Diagrama de classes do gerente:


cd Diagrama de classes do gerenciador
HostProtegido
Host
Permissao
TFormAplicacao

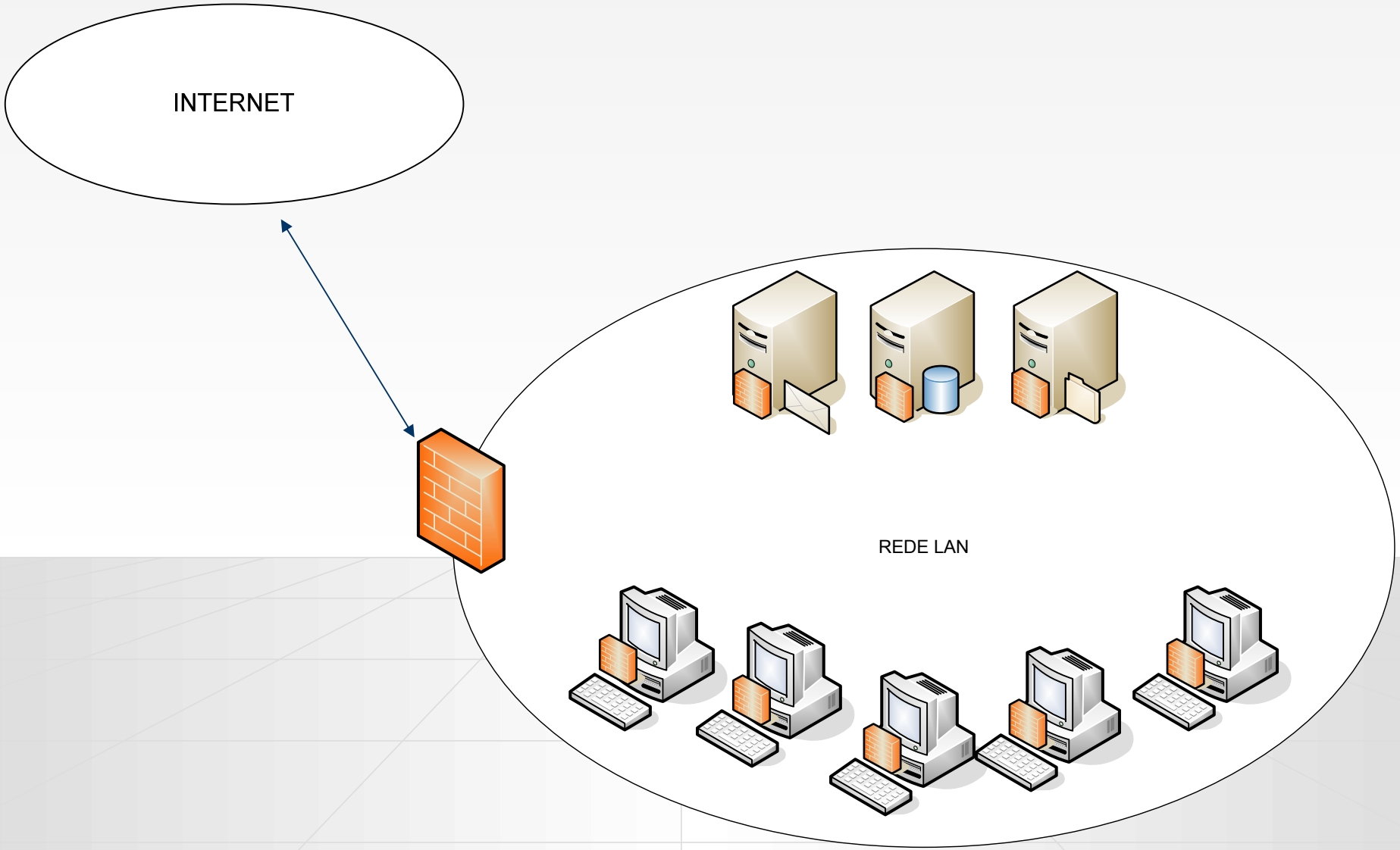
# Desenvolvimento

- Implementação:
  - Principais dificuldades encontradas:
    - Winpcap totalmente compatível com MS Visual C, porém com o Borland foi necessário realizar ajustes em bibliotecas;
    - Utilização do Winpcap através da função CALBACK;
    - Controle do tráfego de mensagens pelo SOCKT;
    - Controle do firewall do Windows através de linha de comando.

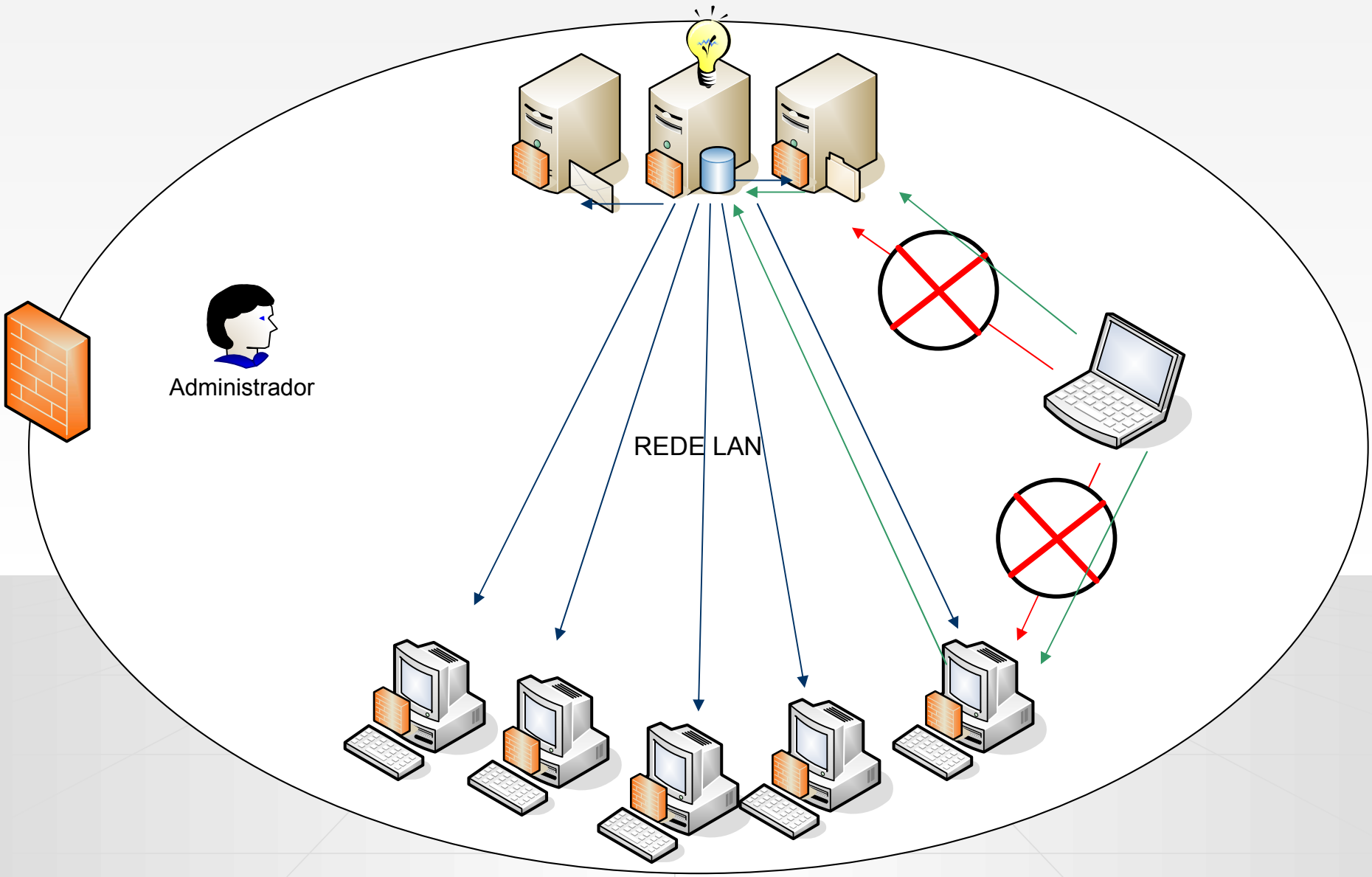
# Desenvolvimento

- Validação:
  - Êxito no cadastro e distribuição de  regras de firewall nas estações protegidas;
  - Êxito ao gerenciar o firewall do Windows XP SP2;
  - Êxito no gerenciamento de bloqueios dos firewalls das estações;
  - Implementado o gerenciamento de troca de endereços IP com algumas ressalvas quanto ao host visitante;
  - Implementado controle de endereço MAC versus endereço IP com algumas ressalvas;
  - Não foi conseguido implementar os relatórios devido a atrasos durante a codificação das demais funcionalidades.

# CONTROLE DE ACESSO A REDE LAN
# VISÃO GERAL



# CONTROLE DE ACESSO A REDE LAN
# VISÃO GERAL



# Conclusões

- É possível realizar controle de acesso a rede LAN através do endereço MAC, utilizando o firewall nativo da Microsoft somado ao componente WINPCAP;
- Tornaria o processo mais simplificado se o firewall do MS Windows permitisse criar regras por endereço MAC, conforme o software IPTABLES encontrado no ambiente LINUX;

# Conclusões

- Devido a características dos roteadores, este sistema não é funcional no controle e gerenciamento de hosts encontrados em uma rede WAN;

# Extensões

- Adapatação do software NetDefender (código aberto) para utilização de regras por MAC;
- Criar no gerenciador método de consultar todas as regras aplicadas em um determinado firewall em tempo real;
- Criar agentes para hosts LINUX, e estações Windows com versões mais antigas como 2000 e 98.