Dividir para Proteger

Daniel de Angelis Cordeiro - 3286158
Danilo Toshiaki Sato - 3313018
Fábio Henrique Nishihara - 3286210

2 de outubro de 2002

Objetivo

Aumentar a segurança de uma grande rede dividindo-a em sub-redes, onde os serviços são providos por servidores locais.

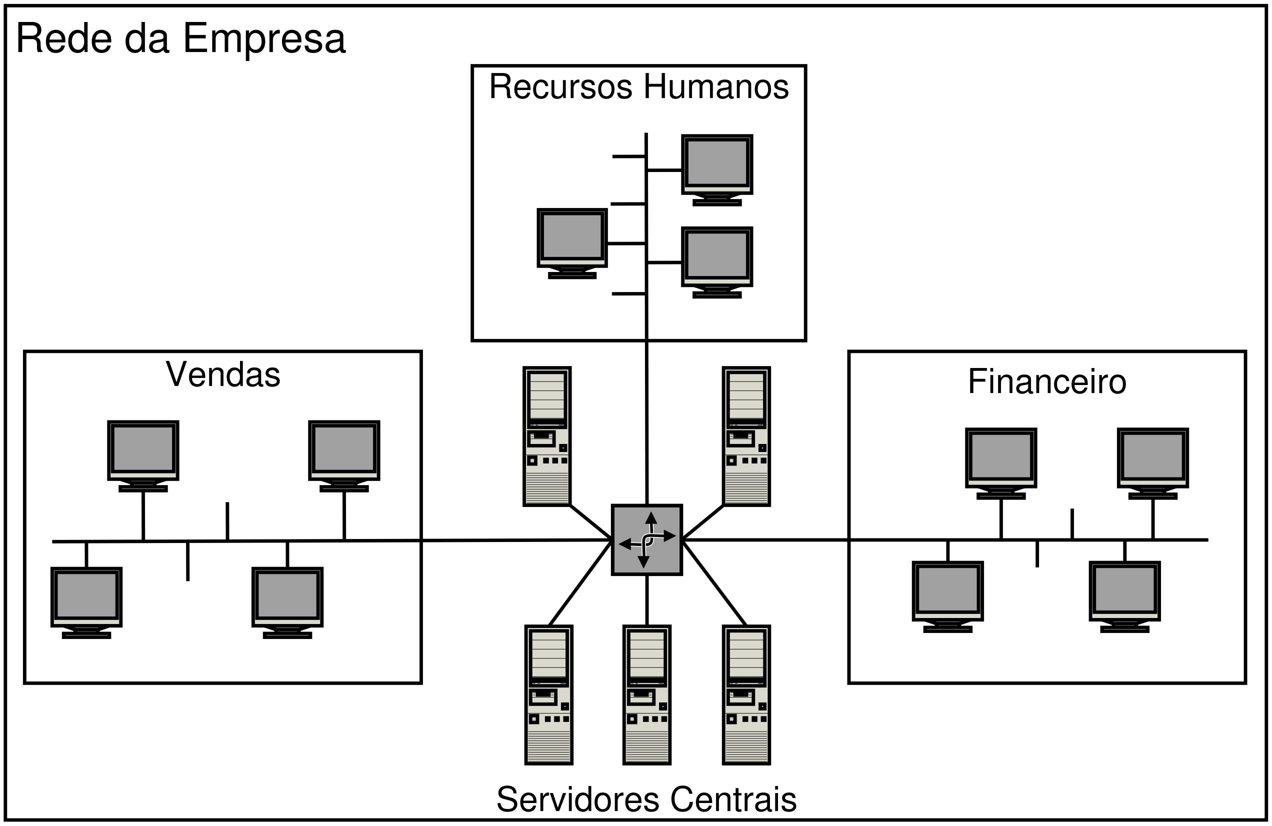
Motivação

A confidencialidade dos dados é um problema que preocupa todas as grandes empresas. Algumas informações de departamentos específicos não podem trafegar livremente por qualquer parte da rede. Além disso, as informações pessoais - como login e senha - dos usuários de cada departamento não podem ser compartilhadas por toda a empresa.

Uma possível arquitetura para esta rede seria disponibilizar um ou mais servidores centrais, que seriam responsáveis por prover os serviços necessários para toda a rede. Porém, pelos motivos acima citados isto tornaria mais fácil o acesso à informações confidenciais por algum usuário não autorizado.

O Padrão Dividir para Proteger sugere que a rede seja dividida em várias sub-redes (uma para cada departamento por exemplo), cada uma com um ou mais servidores locais. Desta forma, serviços específicos de cada departamento são separados não apenas logicamente como também fisicamente, garantindo maior segurança sobre o tráfego de informações na rede como um todo.

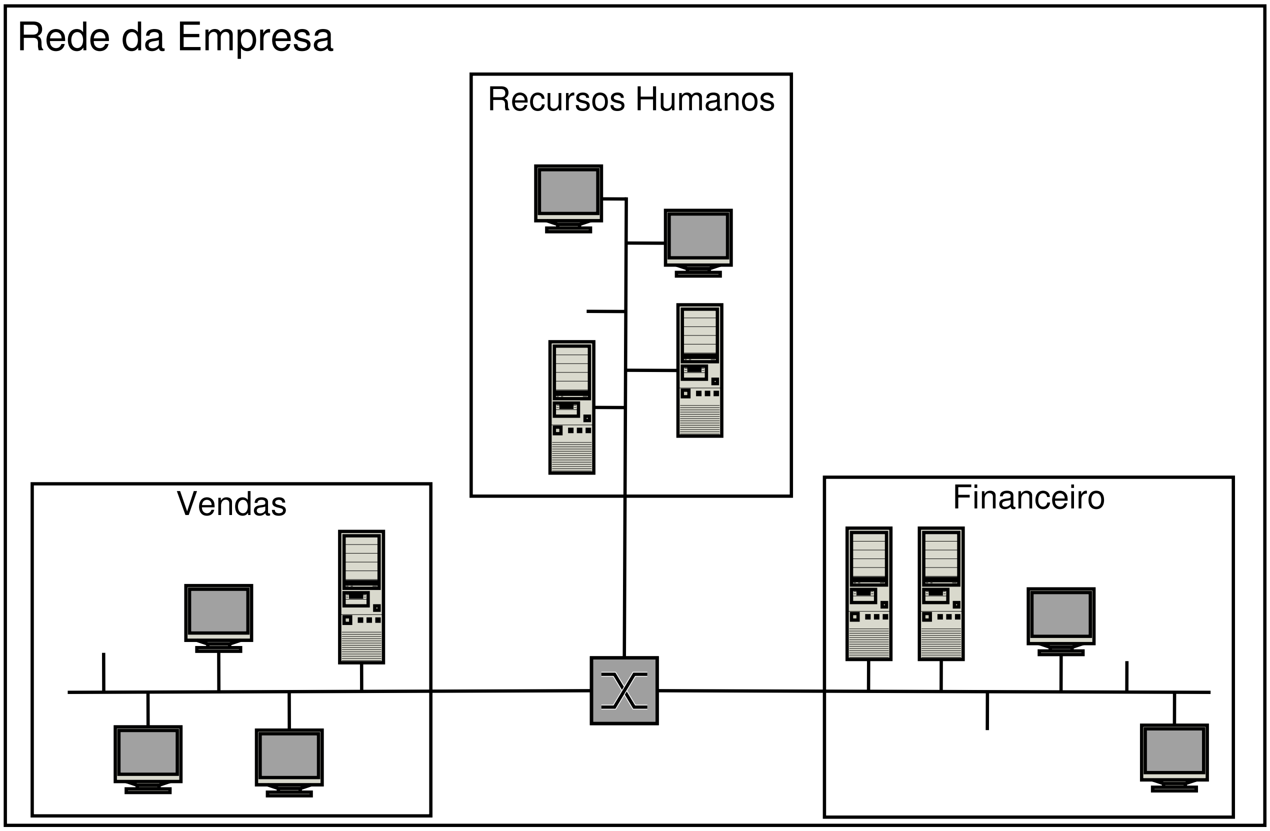
Vamos pegar como exemplo a rede de uma empresa, estruturada conforme a figura abaixo, que possui os seguintes departamentos: Financeiro, Recursos Humanos e Vendas.



Como podemos ver, todos os servidores da rede estão centralizados. Isto causa uma sobrecarga no roteador e, conseqüentemente, perda de desempenho na troca de informações. Outro grande problema desta arquitetura é que um pacote pode trafegar livremente entre qualquer estação, independentemente do departamento ao qual pertence, aumentando a probabilidade de um ataque interno.

Como segurança é um aspecto primordial na rede desta empresa, os arquivos referentes ao departamento Financeiro não podem ser visualizados por qualquer usuário da rede. Da mesma forma, um usuário do departamento de Recursos Humanos não pode acessar informações do departamento de Vendas.

O padrão Dividir para Proteger sugere que esta rede seja subdividida em três sub-redes: uma para cada departamento, cada uma responsável por disponibilizar servidores de arquivos, de autenticação, de impressão, entre outros para seus respectivos usuários. A figura seguinte mostra uma possível arquitetura para essa rede, seguindo o padrão Dividir para Proteger:



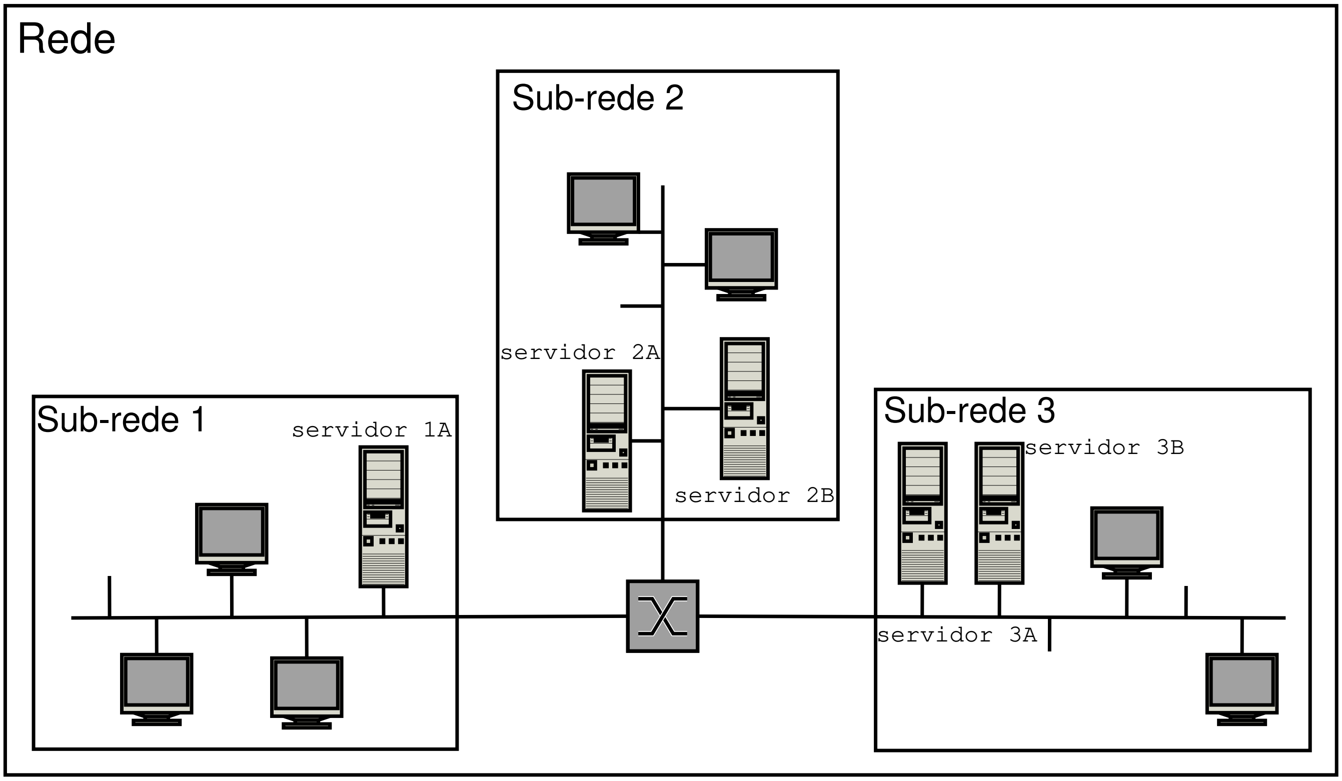
Podemos notar que as estações de trabalho de cada departamento não "enxergam" a rede inteira, mas apenas o servidor local do seu departamento, diminuindo assim o tráfego de informações entre as sub-redes.

Aplicabilidade

Use o Padrão Dividir para Proteger sempre que sua rede apresentar as seguintes características:

1. Um grande número de estações de trabalho;
2. Uma separação lógica entre os dados compartilhados pela rede (cada sub-grupo tem acesso à informações diferentes);
3. Algumas informações não devem estar disponíveis para todos os usuários da rede, apenas um determinado sub-grupo tem acesso à determinadas informações;

Estrutura



Participantes

- *Sub-redes*: representam cada um dos sub-grupos que compõe uma unidade lógica da rede.
- *Servidores*: computadores locais e dedicados que fornecem serviços aos usuários de uma sub-rede específica.
- *Estações de trabalho*: computadores utilizados pelos usuários da rede.

Conseqüências

O padrão Dividir para Proteger apresenta diversos benefícios:

- *Aumento da segurança na troca de dados entre as sub-redes*: Além da segurança garantida normalmente por software - como Firewall, troca de dados por protocolos seguros (SSH), entre outros - há também uma separação física entre as máquinas da rede, dificultando o acesso de um usuário não autorizado a qualquer terminal.

- *Diminuição do tráfego de dados*: Os dados ficam restritos às sub-redes e não trafegam na rede inteira, melhorando a performance de acesso às informações necessárias.

- *Maior proteção contra danos físicos aos servidores*: A distância física entre os servidores garante que no caso de um acidente como, por exemplo, um incêndio apenas uma pequena parcela das informações sejam perdidas.

O padrão introduz alguns problemas:

- *A administração da rede fica dificultada devido a descentralização dos serviços*: Em uma rede onde os serviços são centralizados o administrador do sistema tem maior controle sobre os serviços providos. Tarefas triviais como remoção de usuários, por exemplo, podem ser dificultadas se ele pertencer a mais de uma sub-rede. Uma possível solução para este problema seria a existência de um administrador para cada sub-rede.

- *Os dados da rede podem ficar redundantes e/ou inconsistentes*: Caso um usuário pertença a mais de uma sub-rede, dados como login e senha podem ser diferentes em cada sub-rede.

Usos Conhecidos

A Rede do IME é um exemplo de utilização deste padrão. É subdividida em diversas sub-redes como, por exemplo:

- Rede GNU/Linux dos Alunos de Graduação

- Rede do Grupo de Pesquisa de Processamento não Linear de Imagens (Vision)

- Rede do Laboratório de Computação Paralela e Distribuída (LCPD)

A Rede GNU/Linux centraliza em seus servidores todas as contas e todos os dados dos alunos de graduação do instituto. Dessa forma um usuário da sub-rede do LCPD, por exemplo, não pode se autenticar e nem ter acesso aos dados mantidos nos servidores da Rede GNU/Linux utilizando apenas a sua conta da sub-rede do LCPD. Salvo exceção dos usuários que tem uma conta em ambas as sub-redes.

Padrões Relacionados

- Arquitetura Cliente-Servidor