Proteção de Perímetro

Matteo Nava[2]
Prof. Dr. Adilson Eduardo Guelfi[1]

(1) Faculdade de Informática de PP
UNOESTE

(2) Laboratório de Sistemas Integráveis
Escola Politécnica da USP

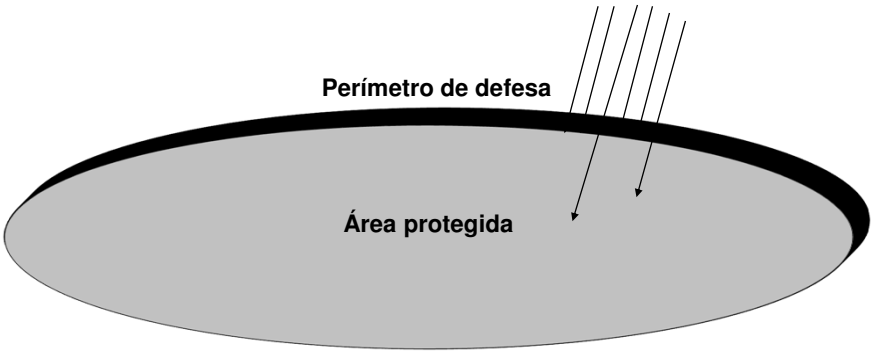
Agenda

- Proteção de Perímetro (PP)
- Exemplo
- Firewall
- Firewall – Classificação
- Filtragem de pacotes
- NAT
- Servidores Bastion Host
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- VPN - Túnel de Segurança
- Referências

Proteção de Perímetro

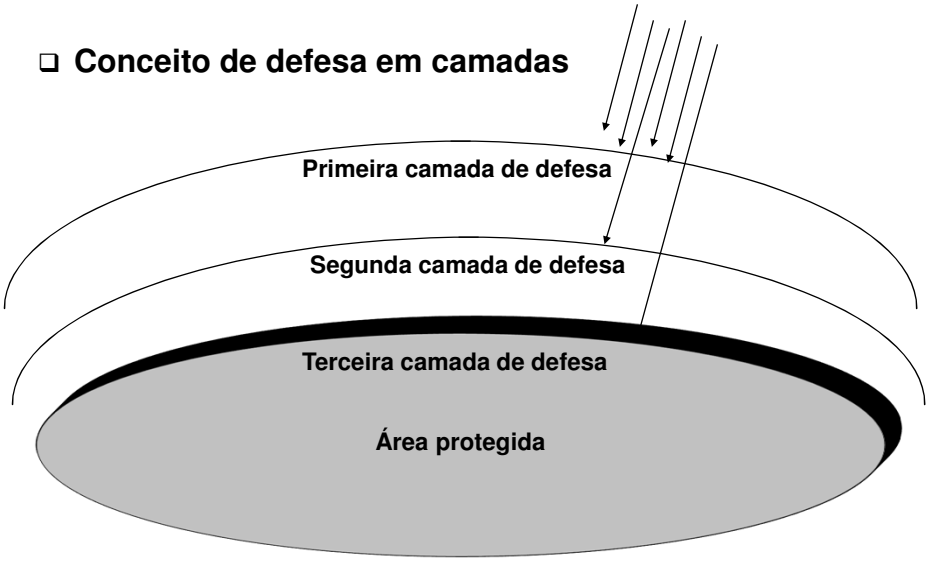
Proteção de Perímetro

- **Conceito de perímetro de defesa**
  - Linha (delimitação) física ou lógica que circunda uma área (área protegida) na qual são aplicados os sistemas ou controles de defesa



Proteção de Perímetro

- **Conceito de defesa em camadas**



Proteção de Perímetro

- **Defesa em camadas**
  - Conceito derivado da área militar, sendo uma das técnicas mais utilizadas para defesa
  - Principais vantagens de se utilizar a defesa em camadas:
    - Impactos dos ataques podem ser melhor absorvidos
    - Uma única camada não é sobrecarregada
    - A eventual falha de uma camada pode ser absorvida por uma outra camada mais interna
    - Ajuda a prevenir observações das posições internas pelo inimigo
  - Cada camada de defesa é composta por:
    - Um perímetro de defesa
    - Sistemas de defesa

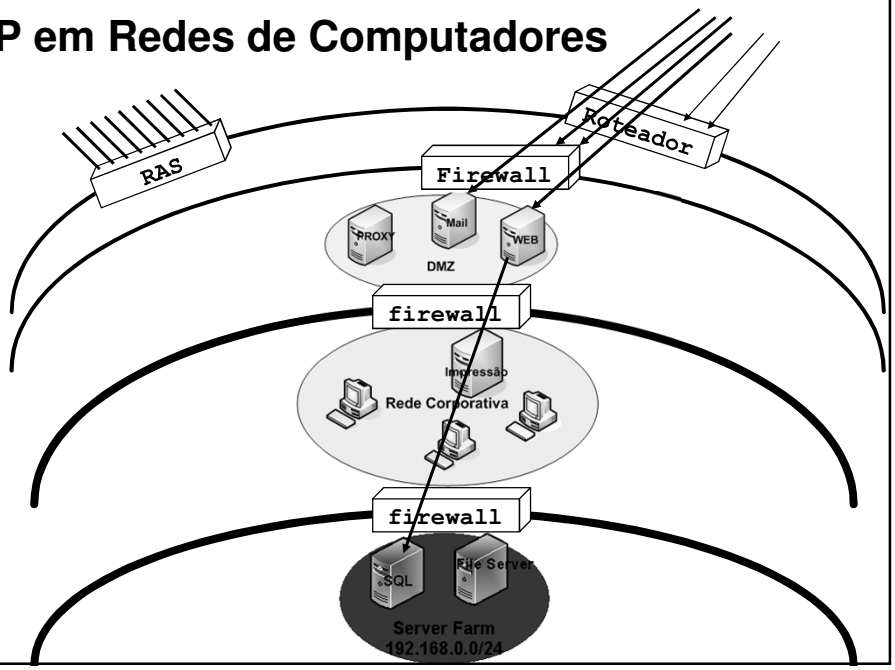
PP em Redes de Computadores

- **Sistemas de defesa**
  - Conjunto de componentes que implementam uma ou mais funcionalidades de proteção
- **Componentes:**
  - Roteador
  - Firewall
  - Sistema Proxy
  - Servidor
  - Sistema de acesso remoto (RAS)
  - Intrusion detection system (IDS)
  - Intrusion prevention sytem (IPS)
  - VPN
  - Switch, HUB
- **Funcionalidades de proteção**
  - Filtragem de pacotes
  - Proxy
  - Geração de registros (logs)
  - NAT
  - Roteamento
  - Bastion Host
  - VPN ou Túnel de segurança
  - Autenticação de usuário
  - Autenticação de parceiro de comunicação
  - Detecção de Intrusão
  - Prevenção de Intrusão
  - VLAN

PP em Redes de Computadores

- **Roteadores**
  - Sistemas especializados em roteamento
  - Não são sistemas especializados em bloqueio
  - Porém, podem implementar funcionalidades de filtragem e NAT
  - Sistemas especializados em defesa devem se encarregar da proteção principal
  - Roteadores e sistemas especializados devem trabalhar de forma cooperativa
- **Firewalls - Sistemas especializados em defesa.**
  - Podem ter disponíveis diversas técnicas de proteção:
    - Filtragem de pacotes
    - NAT
    - Roteamento
    - Proxy
    - Bastion Host
    - Geração de registros (logs)
    - Túnel de segurança ou VPN
    - Autenticação de usuário
    - Autenticação de parceiro de comunicação

PP em Redes de Computadores



PP em Redes de Computadores

Camada	Componentes	Funcionalidades de proteção
Externa	RAS	Autenticação de usuário, registros
	Roteador	Roteamento, filtragem, registros
DMZ	Firewall	Filtragem, VPN (túnel de segurança, autenticação usuário/parceiro), registros
	Servidores DMZ	Bastion Host
Interna	Firewall	Filtragem, registros
Server Farm	Firewall	Filtragem, registros

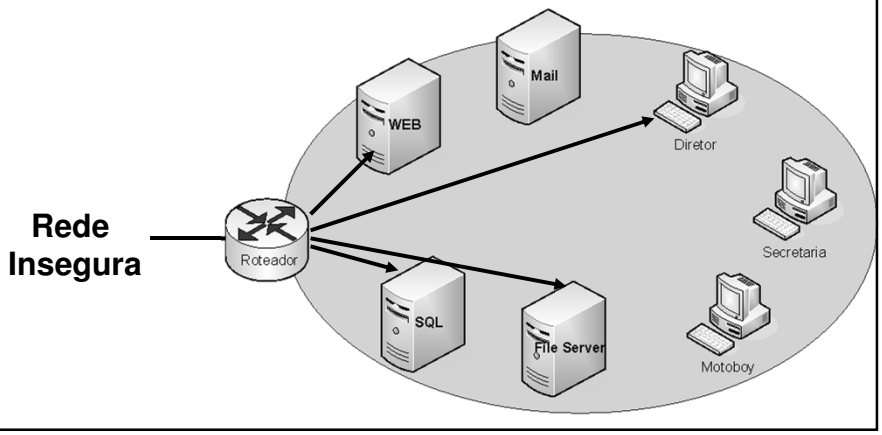
PP em Redes de Computadores

- **Etapas para implantação de proteção de perímetro**
  1. Levantamento dos requisitos de negócio e das necessidades de comunicação
  2. Definição das camadas de segurança
     - Perímetro de segurança
     - Área protegida
  3. Definição do nível de segurança desejado para cada área
     - Critérios
       - Nível de segurança desejado
       - Grau de controle
       - Permissões de acesso
  4. Seleção dos sistemas adequados para cada camada de proteção
  5. Definição das regras de acesso para cada camada de proteção

Exemplo

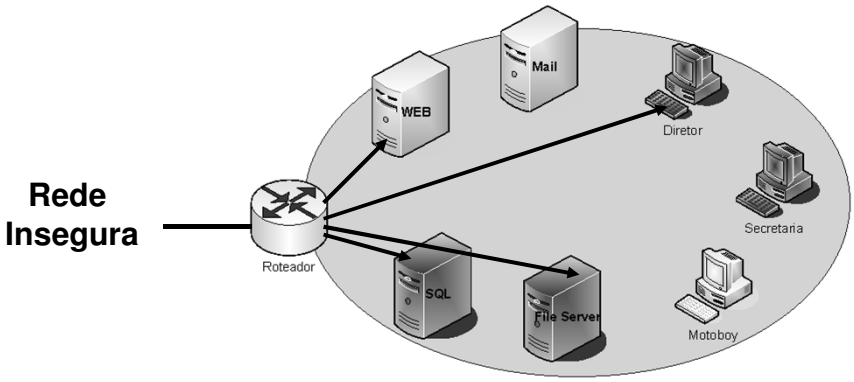
Exemplo

- **Requisitos de negócio e necessidades de comunicação**
  - Identificar a funcionalidade e o papel de cada sistema



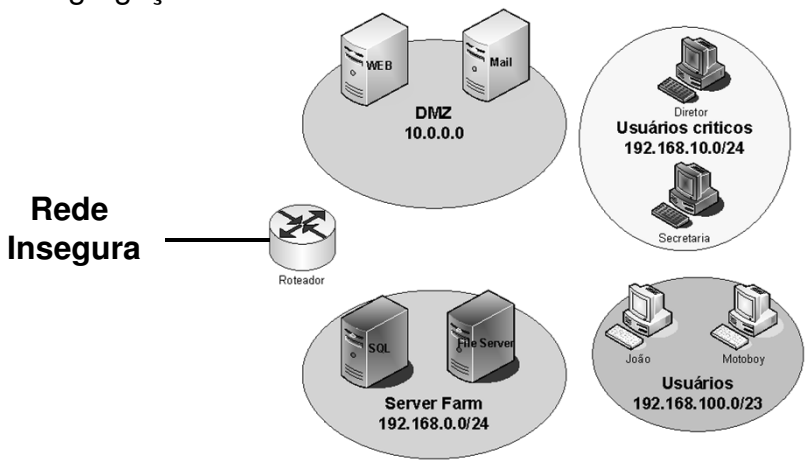
Exemplo

- **Requisitos de negócio e necessidades de comunicação**
  - Identificar os sistemas críticos



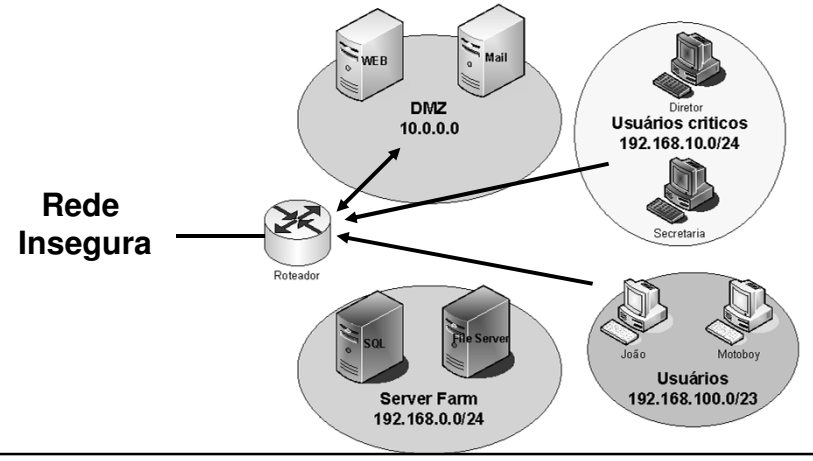
Exemplo

- **Definição das camadas de segurança**
  - Segregação das redes



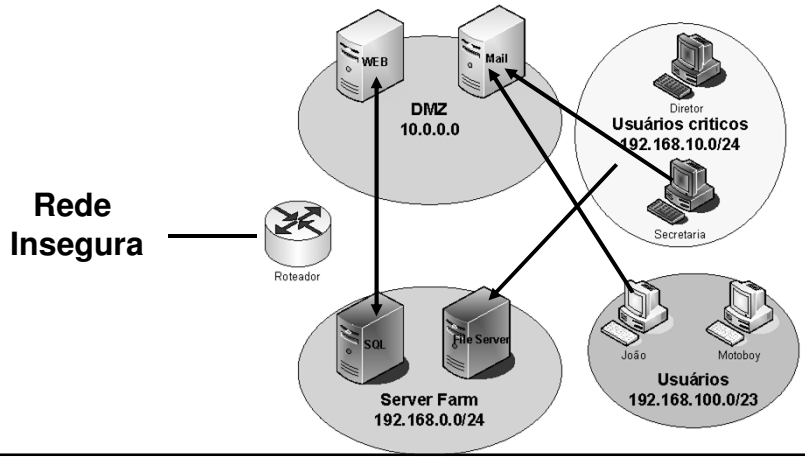
Exemplo

- **Definição do nível de segurança para cada área**
  - Identificar as necessidades de acessos externos
  - Definição dos controles de acesso



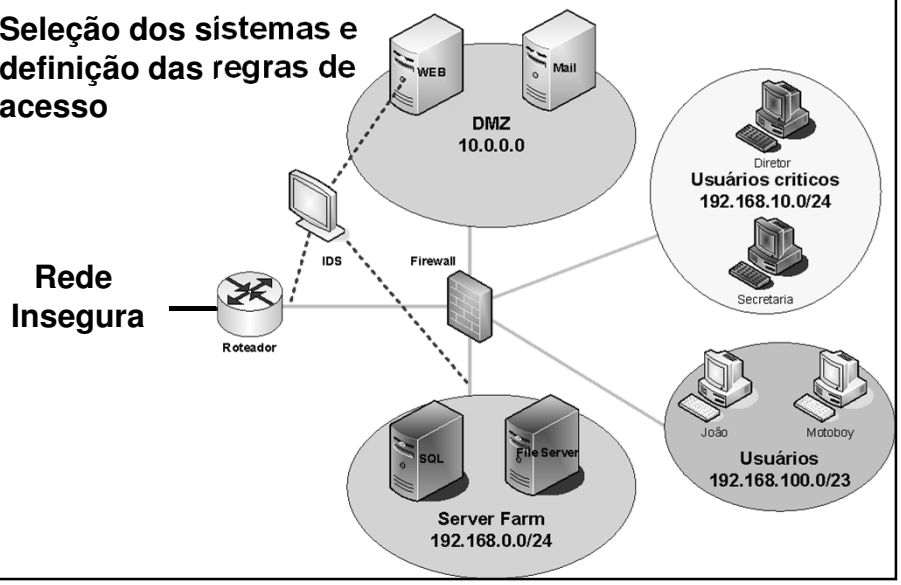
Exemplo

- **Definição do nível de segurança para cada área**
  - Identificar as necessidades de comunicação interna
  - Definição dos controles de acesso



Exemplo

- **Seleção dos sistemas e definição das regras de acesso**



Firewall

Firewall

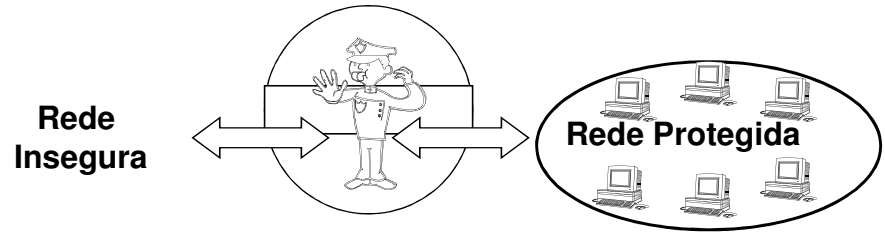
- **Pode se apresentar na forma de**
  - **Software**
    - Programa que é instalado como um serviço em um computador comum (Windows, Unix, Linux)
  - **Hardware ou Appliance**
    - Sistema dedicado para a tarefa de Firewall
    - Pode incluir funcionalidades de filtragem implementadas:
      - Totalmente em software
        - Ex: appliance software Firewall-1
      - Parcialmente em hardware
        - Ex.: Cisco

Firewall

- **O que é?**
  - Sistema in-line
  - Realiza a análise de pacotes que passam por um ponto de rede
  - Permite realizar uma série de ações:
    - Registro (log)
    - Filtragem (aceite, descarte ou bloqueio)
    - Intermediação (Proxy)
    - Estabelecimento de canais seguros (VPN)
    - etc

Firewall

- **Sistema de controle da comunicação, possibilitando:**
  - Posicionar controles de segurança em um ponto de concentração de tráfego da rede
  - Implementar uma política de segurança de restrição de tráfego



Firewall

- **Principais funcionalidades de proteção ou de segurança geralmente disponíveis nos firewalls**
  - Filtragem de pacotes
  - Proxy
  - Roteamento e NAT
  - Túnel de segurança ou VPN
  - Autenticação (usuário e parceiro de comunicação)
- **Controles de segurança adicionais (para pilha TCP/IP)**
  - Controle de fragmentação
  - Proteção contra SYN Flooding
  - Reconstrução do (stream) fluxo de comunicação
  - etc.

Firewall - Classificação

Firewall - Classificação

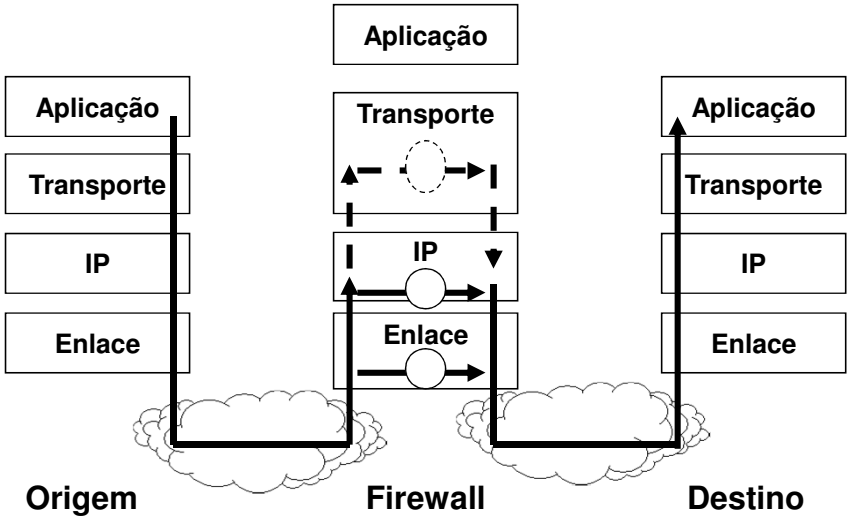
- **Classificação quanto à manutenção de estado**
  - Stateless
    - Não mantém estado da conexão
    - Cada pacote é analisado de forma independente
  - Stateful
    - Mantém estado da conexão
    - O controle de fluxo utiliza o estado da conexão
    - Os pacotes são analisados no contexto de um fluxo de comunicação e não como partes independentes

Firewall - Classificação

- **Classificação quanto à localização da análise de pacotes**
  - Camada intra-rede (ou enlace): Firewall bridge
  - Camada de rede e/ou transporte: Firewall roteador
  - Camada de aplicação: Firewall proxy ou firewall de aplicação

Filtragem de Pacotes

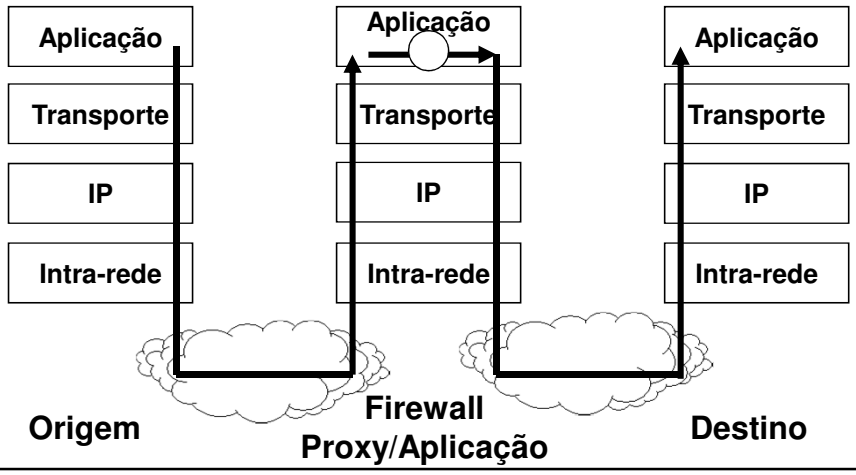
Filtragem: camadas enlace, rede e transporte



Filtragem: camadas enlace, rede e transporte

- **Realiza análise de pacotes sobre**
  - Cabeçalhos de protocolos das camadas de enlace, rede e transporte
  - Interfaces lógicas (IP) de entrada e/ou saída

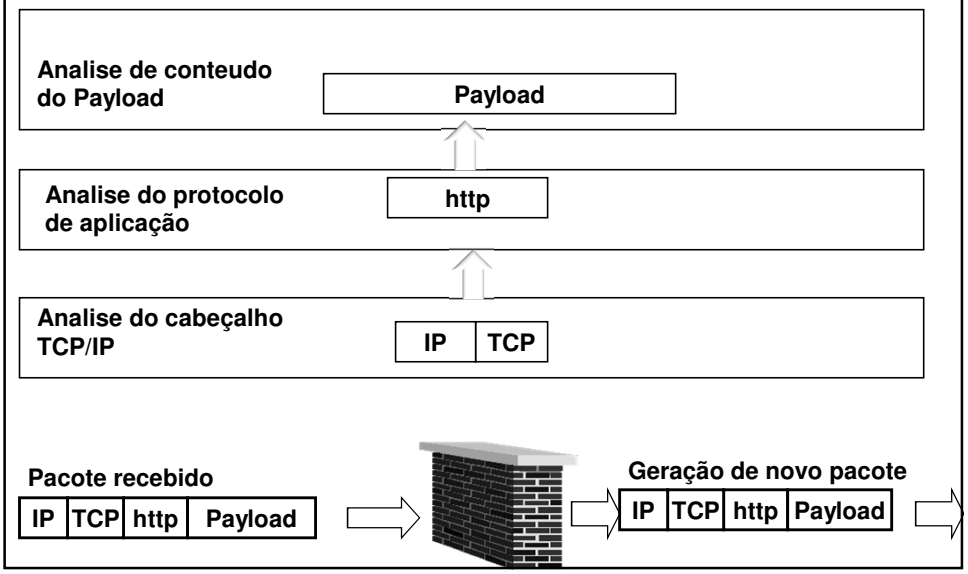
Filtragem na camada de aplicação



Filtragem na camada de aplicação

- **Também denominado de " Firewall Proxy" ou "Firewall de Aplicação"**
- **Realiza análise de pacotes sobre**
  - Cabeçalho de protocolos da camada intra-rede ou enlace
  - Cabeçalhos de protocolos da camada de rede
  - Cabeçalhos de protocolos da camada de transporte
  - Interfaces lógicas (IP) de entrada e/ou saída
  - Protocolos de aplicação (cabeçalho e conteúdo)

Filtragem na camada de aplicação



Filtragem de Pacotes

- **Filtragem na camada de aplicação**
  - Permite maior controle, mas também maior sobrecarga na análise dos pacotes
  - Não propaga vulnerabilidades de protocolos de rede (toda a pilha é processada)
  - Possui capacidade de interpretar conteúdos e tomar decisões sobre os pacotes:
    - permitir/bloquear,
    - redirecionar,
    - modificar e enviar ao destinatário
  - Possui especializações em serviços de rede
  - Funcionalidades adicionais:
    - Cache: armazenar temporariamente as informações
    - Autenticação

Filtragem de Pacotes

- **Filtragem na camada de aplicação**
  - Análise Web - Controles
    - Geração de registros
    - Restrição de
      - Vulnerabilidades (XSS, SQL injection, ...)
      - Sites acessados
      - Aplicações utilizadas (applet, activeX, etc)
  - Analise de E-mail - Controles
    - Podem validar os remetentes, os destinatários, anexos e os textos dos e-mails
    - Black, white e Gray lists (SPAMs)

NAT

NAT

- **NAT**
  - "*Network Address Translation*"
    - Tradução de endereços de rede
  - Método de tradução de
    - Endereço IP
    - Porta TCP/UDP
  - Utilizado principalmente para viabilizar a comunicação com máquinas que utilizam endereços privados
  - Funcionalidade de proteção geralmente realizada por elementos de roteamento

NAT

- **Apesar de não ter sido originalmente criado para prover segurança, o NAT em proteção de perímetro pode contribuir para:**
  - Omitir a topologia de rede interna utilizada em um ambiente
  - Limitar a comunicação de portas TCP/UDP especificas
  - Agregar mais de um sistema de defesa atrás de um único endereço de rede real
  - Servir como ponto de concentração dos pacotes de rede

Bastion Host

Bastion Host

- **Problema:**
  - Instalação default de sistema operacional (e outros sistemas) é concebida para operar sem problemas
  - Não existe preocupação com aspectos de segurança
- **Bastion Host ou Hardening:**
  - Denominação atribuída a sistemas configurados com alto nível de segurança
  - É geralmente utilizado para sistemas expostos a redes inseguras ou redes desmilitarizadas
  - O *Bastion Host* assegura uma configuração de SO mais robusta contra ataques, além de auxiliar na implantação menos complexa de outros sistemas, tais como, o *firewall*

Intrusion Detection System (IDS)

Intrusion Detection System (IDS)

- **Tipo de controle:**
  - Monitoração e Detecção
- **Sistema que**
  - Captura pacotes de um ponto da rede
  - Analisa os comportamentos de rede em busca de comportamentos anômalos
- **Após ter detectado um comportamento suspeito atua:**
  - Gerando um log
  - Disparando um alarme
  - Interagindo com outro sistema para prevenção (bloqueio)

Intrusion Detection System (IDS)

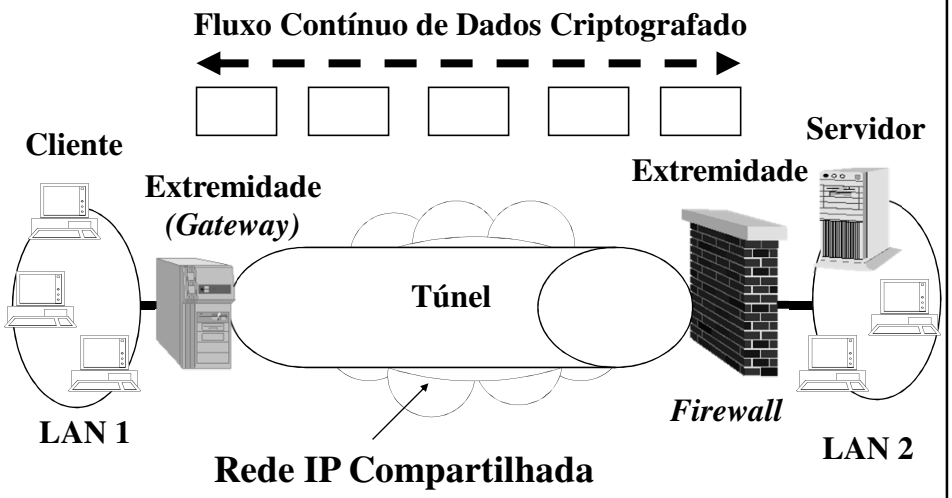
- **Tipos de IDS**
  - Rede
    - Realiza a observação de pacotes de rede
    - Realiza análise do tráfego da rede para identificar padrões considerados suspeitos
  - Host
    - Instalado no servidor
    - Sistema acompanha serviços, processos e logs do sistema

VPN
(Túnel de Segurança)

VPN - Túnel de Segurança

- **Permite que um usuário ou sistema autorizado possa transpor de forma segura uma camada de defesa**
- **Canal seguro de comunicação pode ser implementado entre:**
  - Usuário e outro usuário (cliente-cliente)
  - Usuário e uma rede (cliente-gateway)
  - Rede com rede (gateway-gateway)
- **Utilizado em conjunto com técnicas de autenticação de usuário e/ou autenticação de parceiro**
- **Exemplos**
  - Canal IPSEC (camada de rede)
  - Canal SSL/TLS (camada de transporte)
  - Canal SSH (camada de aplicação)

VPN - Túnel de Segurança



Referências

Referências

- **Hacker Proof**
  - The Ultimate Guide to Network Security
  - **Lars Klander**
- **Building Internet Firewalls**
  - Internet Security
  - **D. Brent Chapman e Elizabeth D. Zwicky**