PROJETO DE REDES
www.projetoderedes.com.br

Segurança da Informação

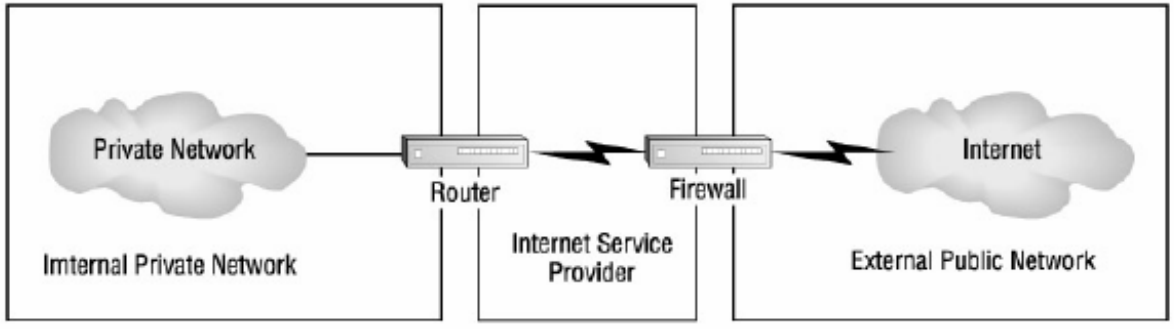
Firewalls e Redes de Perímetro

José Maurício S. Pinheiro - 2008

Firewall - Definição

O Firewall opera nas camadas de transporte e de rede do modelo TCP/IP, tendo como principal finalidade a análise e a filtragem de pacotes.

Um firewall é uma passagem (“gateway”) que restringe e controla o fluxo do tráfego de dados entre redes, mais comumente entre uma rede interna e a Internet. Pode, também, estabelecer passagens seguras entre redes internas.

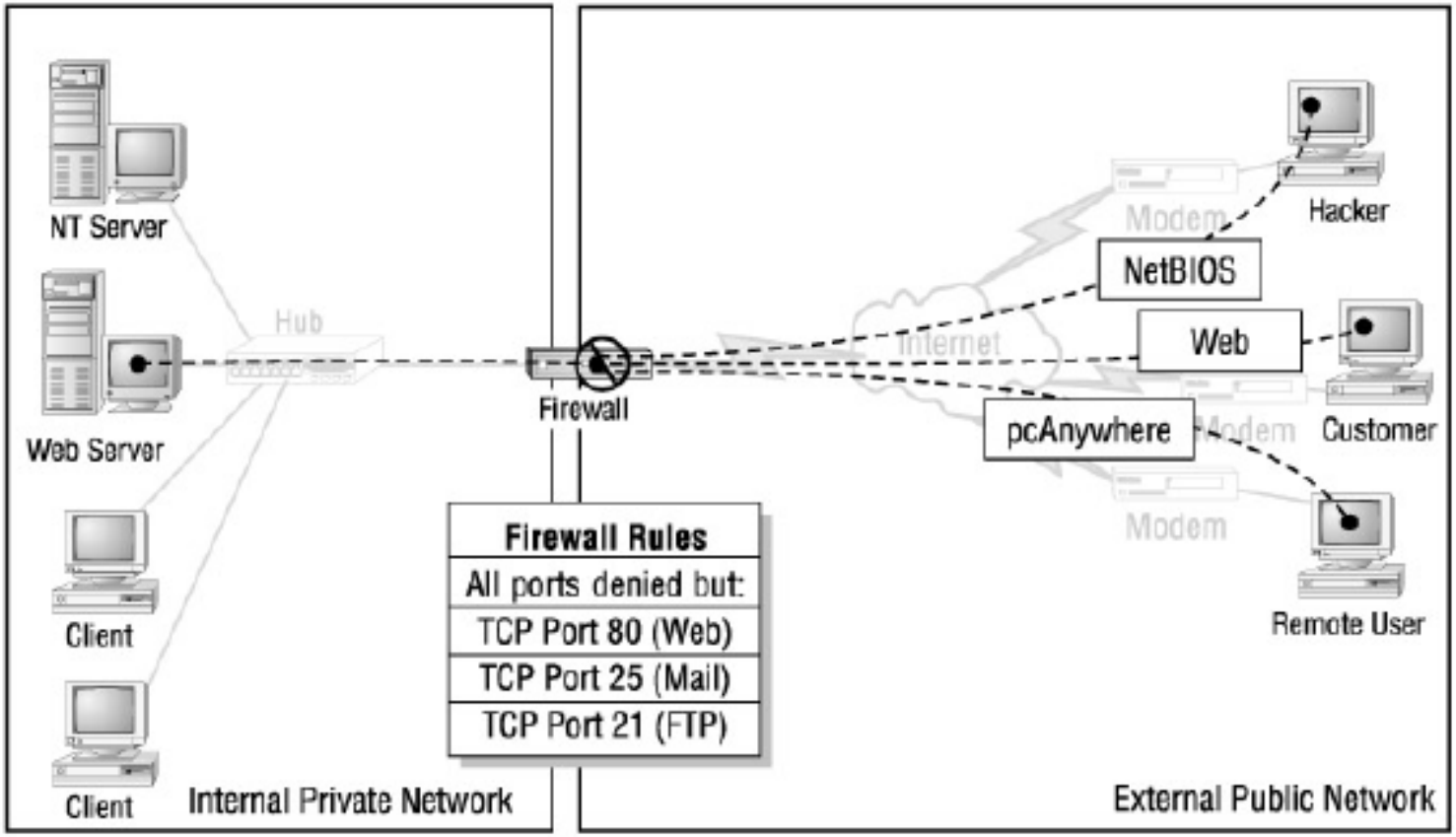


Filtragem do Tráfego no Firewall

- Firewalls simples são baseados em roteadores e filtram o tráfego baseado no endereço de origem, endereço de destino, protocolo, além dos critérios da política de segurança.

- **Firewalls estáticos** - permitem qualquer serviço a menos que ele seja expressamente rejeitado ou rejeita qualquer serviço a menos que ele seja expressamente permitido.
- **Firewalls dinâmicos** - permitem/rejeitam qualquer serviço segundo os critérios da política de segurança da rede.

Filtragem do Tráfego no Firewall



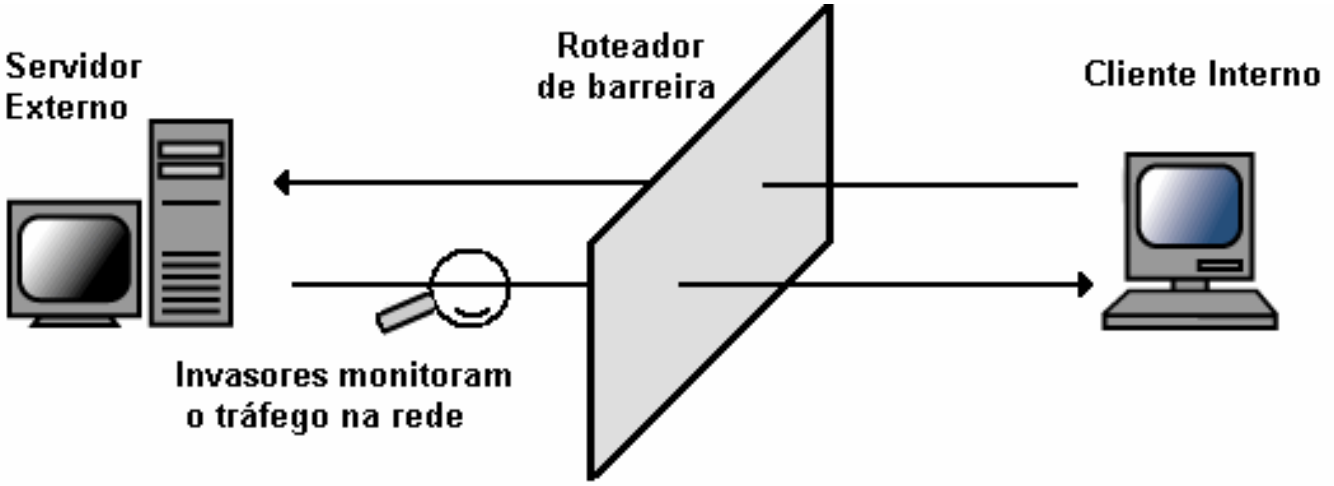
Funções de Firewall

- **Filtro de pacotes** - análise dos cabeçalhos dos pacotes;
- **NAT (Network Translator Address)** - Controla a origem ou destino dos pacotes, alterando no cabeçalho a porta e/ou endereço IP do pacote, seja de origem ou de destino, conforme a necessidade;
- **Híbridos** - Associam a função de filtragem de pacotes e a função NAT.

Tipos de Firewall

1. Roteador de Barreira (Packet Filtering)

Consiste de recursos implementados no roteador da rede. O roteador pode ser um equipamento específico ou um computador com duas placas de rede, que filtra os pacotes baseando-se no endereço IP ou no tipo de conexão.



Tipos de Firewall

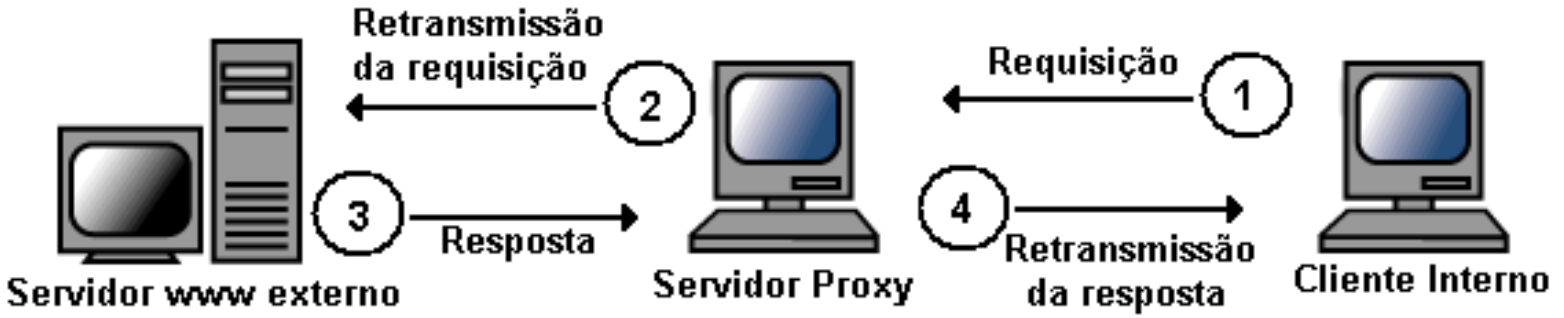
2. Gateway de Servidor Proxy (Application Proxy)

- Entrega mensagens de um cliente interno a um serviço externo. O Proxy muda o endereço IP dos pacotes do cliente para protegê-lo na Internet; o único endereço que vai para a Internet é o do Proxy.
- O Proxy diminui as possibilidades de um hacker obter informações sobre os computadores da rede interna. Ele esconde o endereço IP de todos os computadores da rede interna.

Tipos de Firewall

Dois tipos de Servidores Proxy

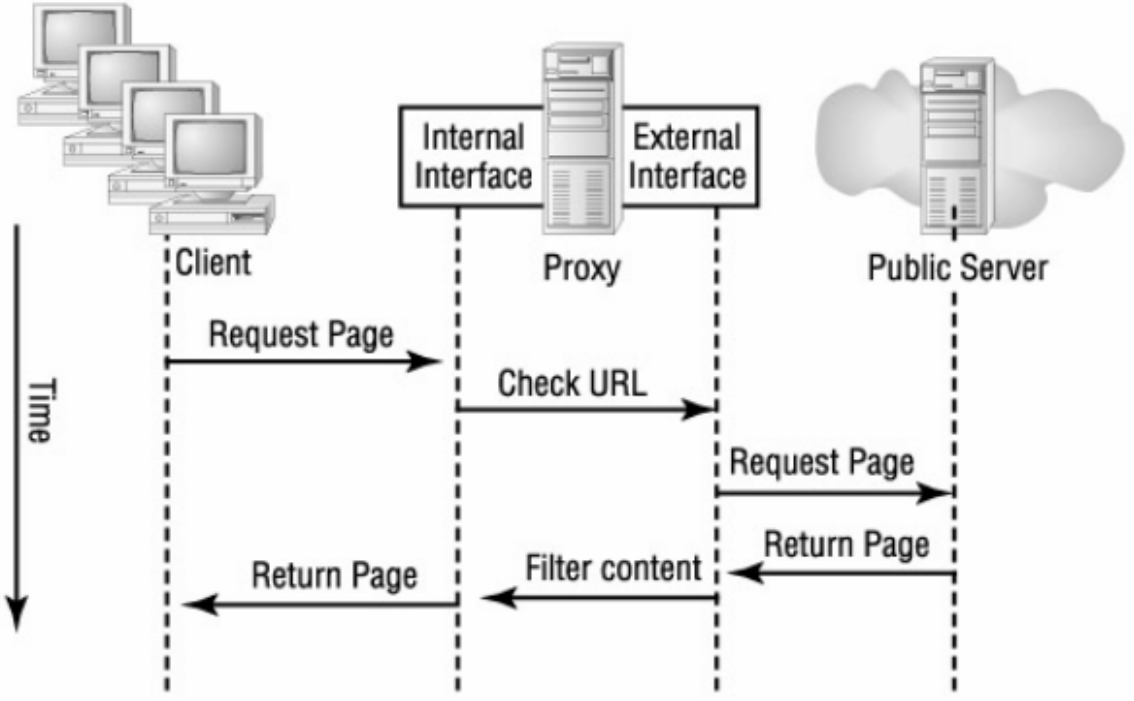
- **Gateway de Nível Circuito** - provê conexão controlada entre sistemas internos e externos (existe um circuito virtual entre os clientes e o Proxy). O sistema interno e o externo nunca se conectam, senão através do Proxy.



Tipos de Firewall

Dois tipos de Servidores Proxy (cont)

- **Gateway de Nível Aplicação -** serviços básicos e análise dos pacotes; o pacote é examinado e avaliado e a política de segurança permite ou não que este entre na rede interna.



Bastion Host

- Conhecido como “Application Gateway” - por definição é qualquer máquina configurada para desempenhar algum papel crítico na segurança da rede interna;

- Máquina segura, localizada no lado público da rede de perímetro (acessível publicamente), mas que não se encontra protegida por um firewall ou um roteador de filtragem, expondo-se totalmente a ataques.

Bastion Host

- Configurado de forma que serviços, protocolos, programas e interfaces de rede desnecessários são desabilitados ou removidos;
- Cada bastion host é usado para uma função específica.
- Firewalls mais sofisticados empregam bastion host como servidor proxy, evitando acesso direto dos usuários à Internet, filtrando entradas não autorizadas de tráfego da Internet.

Bastion Host

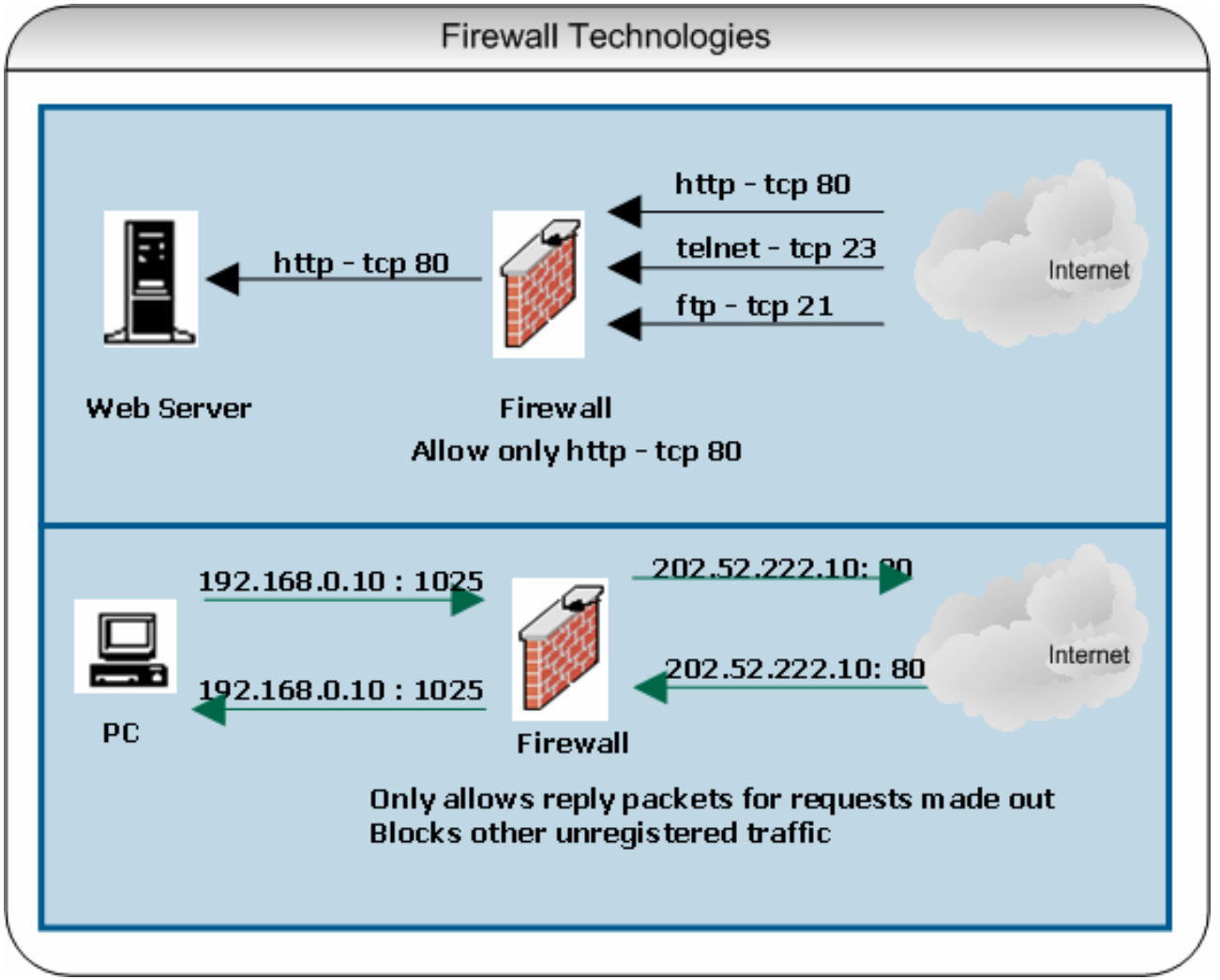
- Bastion hosts limitam potenciais ataques. Por esse motivo são um ponto crítico na segurança da rede, necessitando de cuidados extras como auditorias regulares.

Tipos de Firewall

3. Gateway de Técnicas de Inspeção de Estado (Stateful Inspection)

- No lugar de examinar cada pacote, compara o padrão de bits do pacote com um padrão conhecido como confiável. o Firewall compara o pacote recebido com o estado salvo para definir se ele está autorizado a entrar.
- A técnica fornece transparência e velocidade, mas uma das desvantagens é que pacotes internos podem acessar a rede externa com seus próprios endereços IP, expondo a rede interna a ataques.

Tipos de Firewall



Tipos de Firewall

4. Gateway Sentinela (Guard)

- Firewall sofisticado que analisa os dados segundo o protocolo e decide quais serviços podem ser executados na rede interna de acordo com as regras estabelecidas pela política de segurança.
- O grau de controle que o sentinela pode prover é limitado pelas determinações das políticas de acesso. Porém pode adquirir funcionalidades semelhantes aos servidores proxy.

Tipos de Firewall

5. Firewall Pessoal (Personal Firewall)

- Tipo específico de firewall - trata-se de um software ou programa utilizado para proteger um computador contra acessos não autorizados vindos da Internet.

- Um firewall pessoal bem configurado pode bloquear tentativas de invasão, podendo barrar também o acesso a backdoors, mesmo se já estiverem instalados no computador.

Tipos de Firewall

5. Firewall Pessoal (cont.)

- Alguns programas de firewall permitem analisar continuamente o conteúdo das conexões, filtrando vírus de e-mail, cavalos de tróia e outros tipos de malware, antes mesmo que o antivírus entre em ação.

- Existem pacotes que funcionam em conjunto com os antivírus, provendo maior segurança para os computadores onde são utilizados.

Registro de Eventos

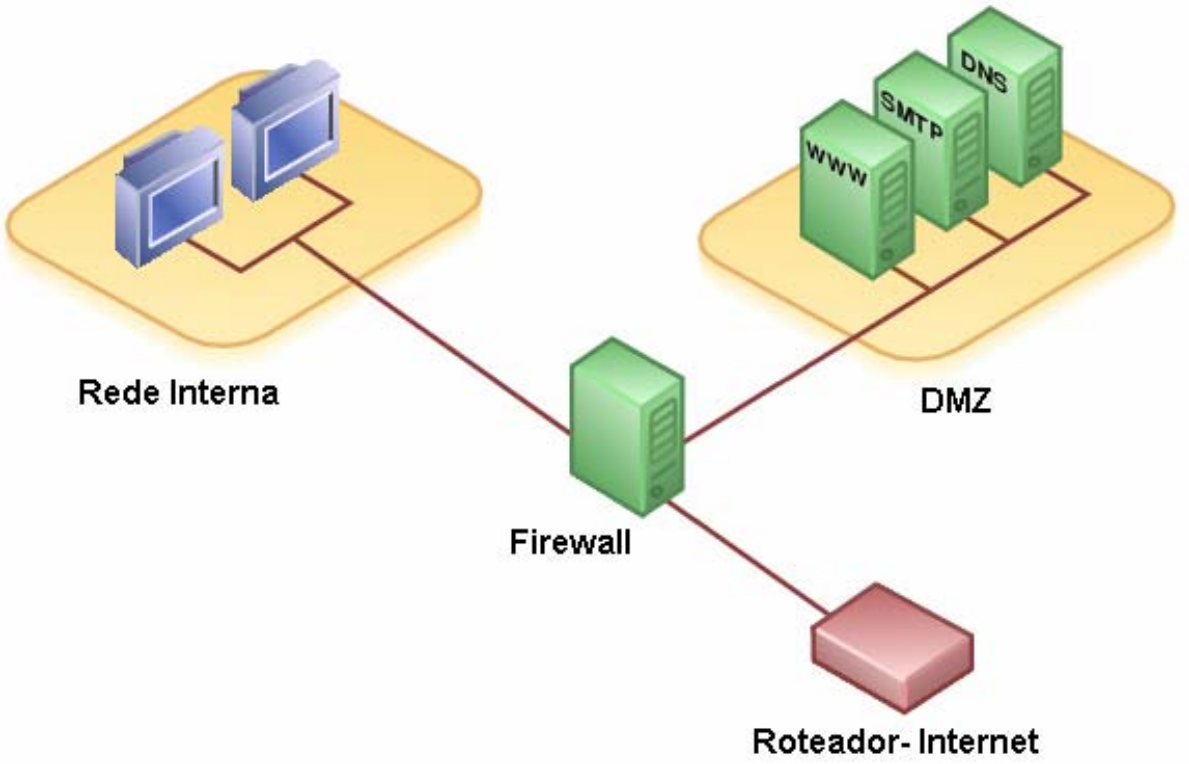
- **Log's** - registros de atividades gerados por programas de computador. No caso de log's relativos a incidentes de segurança, eles normalmente são gerados por **Firewalls** ou por Sistemas de Detecção de Intrusão (IDS).
- O Firewall pode gerar logs quando um acesso é negado. Esse acesso pode ser considerado uma tentativa de invasão, mas também pode ser um falso positivo (aponta uma atividade como sendo um ataque, quando na verdade esta atividade não é um ataque).

Registro de Eventos

- Os logs relativos a ataques, em geral, apresentam as seguintes informações:
    - Data e horário em que ocorreu uma determinada atividade;
    - Endereço IP de origem da atividade;
    - Portas envolvidas;
    - Time zone (fuso horário) do log;
    - Protocolo utilizado (TCP, UDP, ICMP, etc);
    - Os dados enviados para o computador ou rede.

Rede de Perímetro

O Firewall oferece a opção de criar uma zona de vigilância na rede mais fraca, conhecida como DMZ, Rede de Perímetro ou Zona Neutra.



Rede de Perímetro

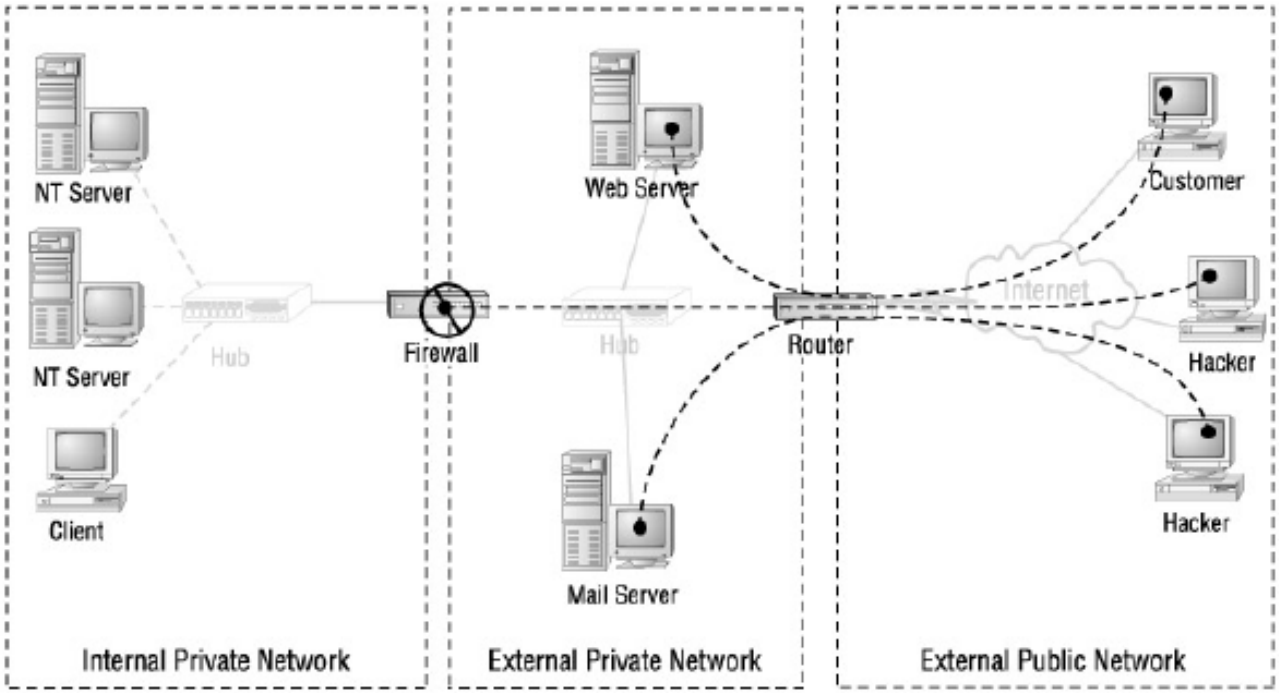
Rede de Perímetro refere-se a um segmento de rede isolado no ponto em que uma rede corporativa alcança a Internet.

As redes de perímetro destinam-se a criar um limite para permitir a separação do tráfego entre redes internas e externas. Os serviços e servidores que devem interagir com a rede externa (desprotegida) são colocados na rede de perímetro (conhecida como zona desmilitarizada) e na sub-rede filtrada.

Rede de Perímetro

Dois tipos:

- **Interna** - acessada somente pela rede interna;
- **Externa** - acessada por qualquer usuário da rede externa (Internet).



Rede de Perímetro

• A DMZ comporta-se como uma sub-rede (atrás do firewall), onde uma máquina segura na rede externa (que não executa nenhum serviço), avalia as requisições e encaminha cada serviço para a máquina destino na rede interna;

• Hospeda os servidores/serviços protegidos contra ataques externos via firewall.

• É necessário especificar uma faixa de endereços IP, ou informar diretamente os endereços das máquinas que devem ser incluídas nessa zona.

Rede de Perímetro

A DMZ pode incluir regras de acesso específico e sistemas de defesa de perímetro para que simule uma rede protegida, induzindo possíveis invasores para armadilhas virtuais (honeypots).