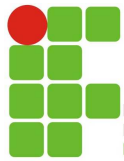
Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Técnicas de Defesa
(Firewall)



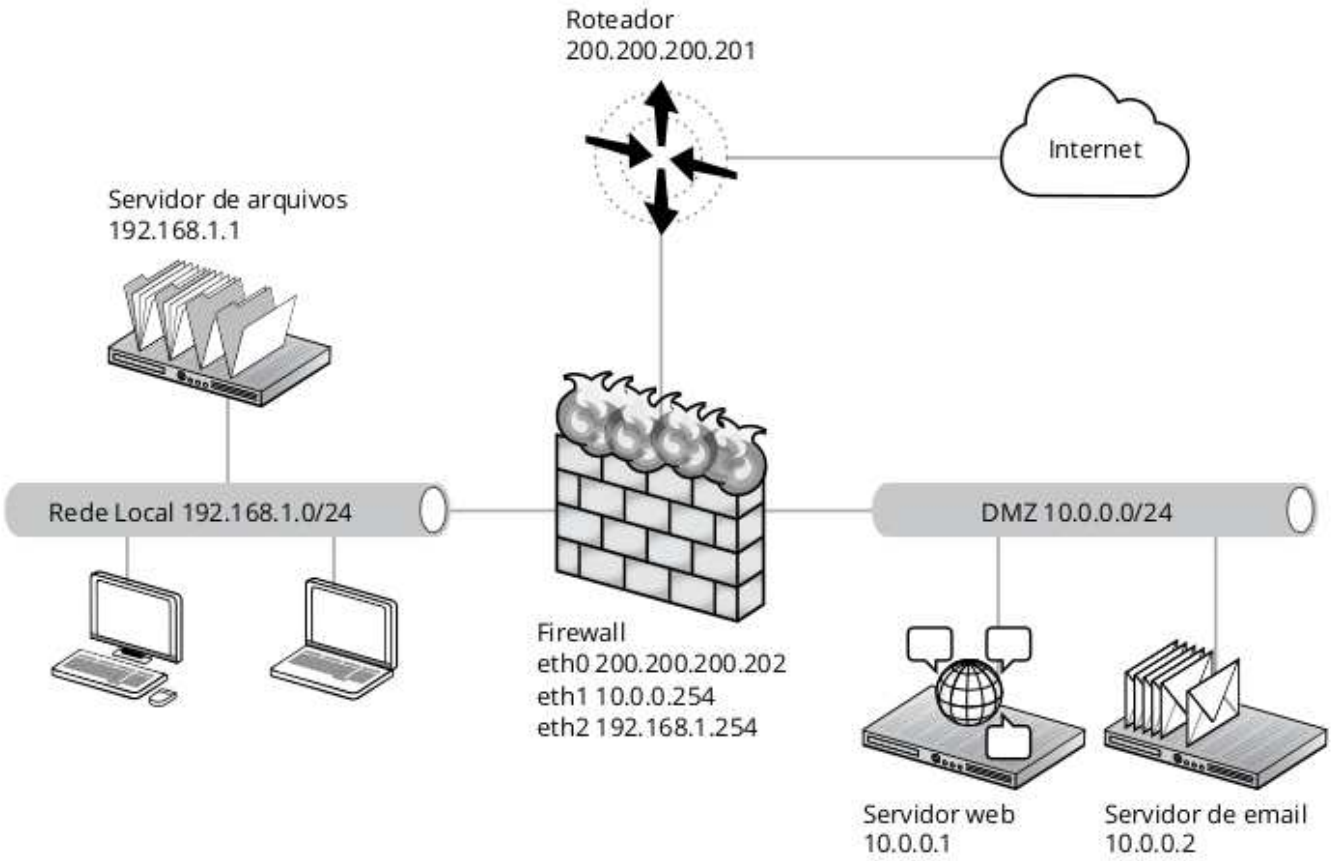
INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Introdução

O firewall é um dispositivo de segurança (normalmente um roteador ou um computador) instalado entre a rede interna de uma organização e o restante da Internet para estabelecer uma ligação **controlada** e montar um muro ou perímetro de segurança externo. A meta desse perímetro é proteger a rede corporativa contra **ataques provenientes da Internet** e prover um **único ponto de entrada/saída** no qual segurança e **auditoria** possam ser impostas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução



Intercepta todo o tráfego de entrada e saída da rede

Introdução

Características

- Fisicamente pode ser um roteador, um computador ou uma combinação de roteadores e computadores com o software apropriado;
- Somente tráfego autorizado, como definido pela política de segurança local, terá permissão de passar;
- Facilita a auditoria da rede;
- Proteger uma rede privada contra "intrusos";
- Impedir envio de informações não autorizadas;
- Bloquear acesso a sites particulares;
- Prevenir que certos usuários/máquinas acessem certos servidores/serviços;
- É transparente aos usuários.

Introdução

Existem firewalls baseados na combinação de hardware e software e firewalls baseados somente em software. Este último é o tipo recomendado ao uso doméstico e também é o mais comum.

Também, temos os Firewalls Home, destinados a uma máquina ou uma estação de trabalho (workstation). Ele controla os dados que entram e saem da máquina.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução

O firewall também é adequado para:

- Implementação de serviços como NAT e VPN;
- Realização de auditorias; e
- Geração de estatísticas do uso da rede.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Introdução

Tecnologias de firewall

- Filtro de pacotes (Packet Filter);
- Filtro de pacotes baseado em estados (StatefulPacket);
- Proxy.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtro de Pacote

De acordo com um conjunto de regras pode negar o pacote (DROP) ou deixar o pacote passar (ACCEPT) com base nas informações contidas em cabeçalhos da camada de rede ou de transporte, por exemplo, endereços IP de origem e de destino, endereços de porta de origem e de destino e o tipo de protocolo (TCP ou UDP).

Um firewall de filtragem de pacotes usa uma tabela de filtragem para decidir quais pacotes devem ser descartados (não encaminhados).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Filtro de Pacote

A sequência na qual as regras são aplicadas pode alterar completamente o resultado da política de segurança. Por exemplo, as regras de negação incondicional devem ser sempre as últimas regras da lista.

Ação	Direção	Protocolo	IP Origem	IP Destino	Porta Origem	Porta Destino	ACK
permitir	Out	tcp	interno	*	> 1023	23	*
permitir	In	tcp	*	interno	23	> 1023	1
permitir	In	tcp	*	interno	> 1023	23	*
permitir	Out	tcp	interno	*	23	> 1023	1
negar	*	*	*	*	*	*	*

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Filtro de Pacote

Os filtros de pacotes também são chamados de *stateless* firewall. Cada pacote é tratado de forma isolada, ou seja, não guarda o estado da conexão e não sabe se o pacote faz parte de uma conexão feita anteriormente.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Filtro de Pacote Baseado em Estados

Filtro de pacotes dinâmicos ou baseado em estados, decisões de filtragem usando informações dos cabeçalhos dos pacotes e uma tabela de estados, que guarda os estados de todas as conexões. Guardam na memória o estado das conexões.

O firewall trabalha verificando somente o primeiro pacote de cada conexão. Se este pacote é aceito, os demais pacotes são filtrados de acordo com as informações desta conexão na tabela de estados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

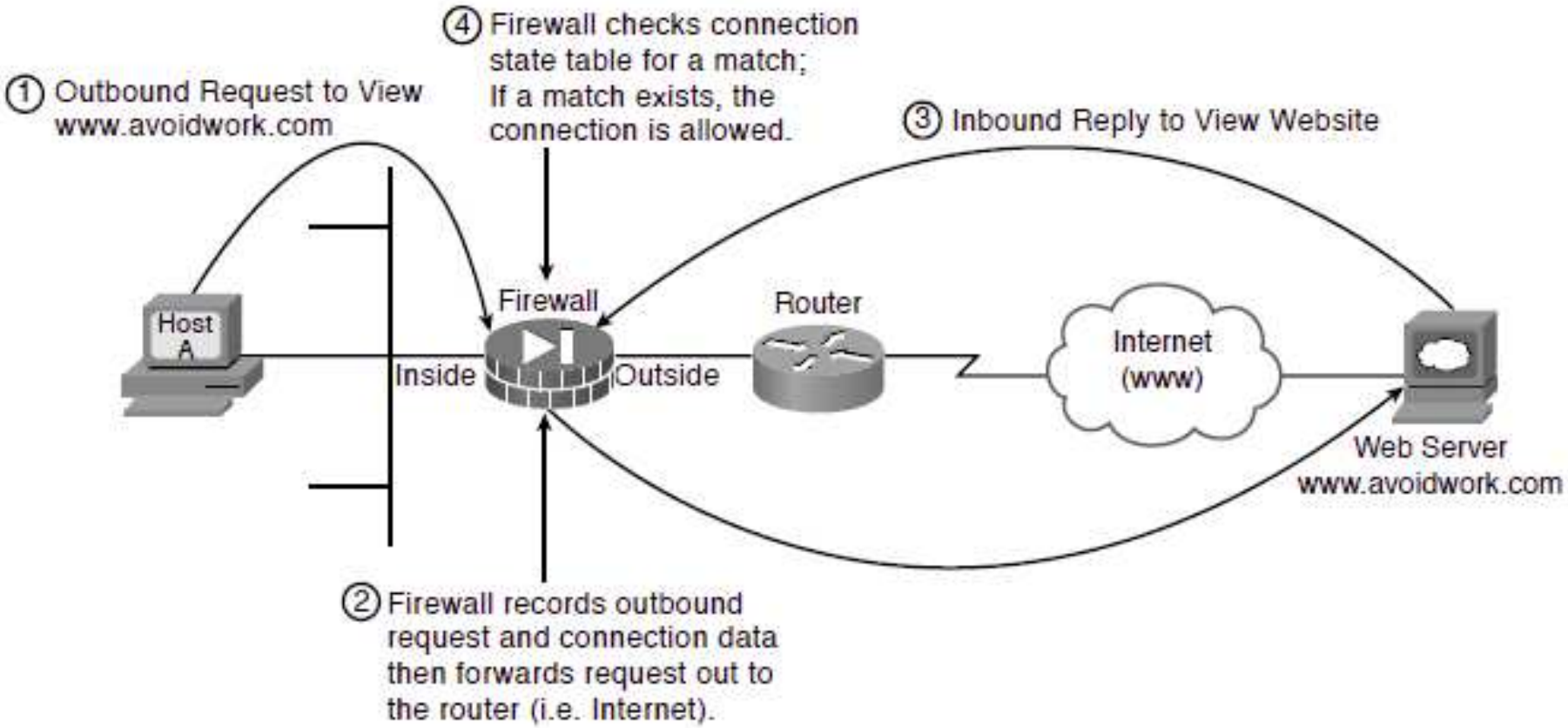
Filtro de Pacote Baseado em Estados

Por exemplo, quando um host interno inicia a conexão solicitando alguma informação de um servidor externo, o firewall aguarda por uma resposta daquele servidor específico destinado ao host que iniciou a conexão e a uma porta específica. Quando a resposta retorna, a entrada do pacote é autorizada, mesmo que não haja uma regra específica autorizando aquele endereço IP.

Se algum pacote é encaminhado à rede sem ter sido requisitado por um host interno, a entrada do mesmo é negada, mesmo que, nas regras, aquele endereço IP seja autorizado, deixando, assim, a rede menos vulnerável a ameaças.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Filtro de Pacote Baseado em Estados



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

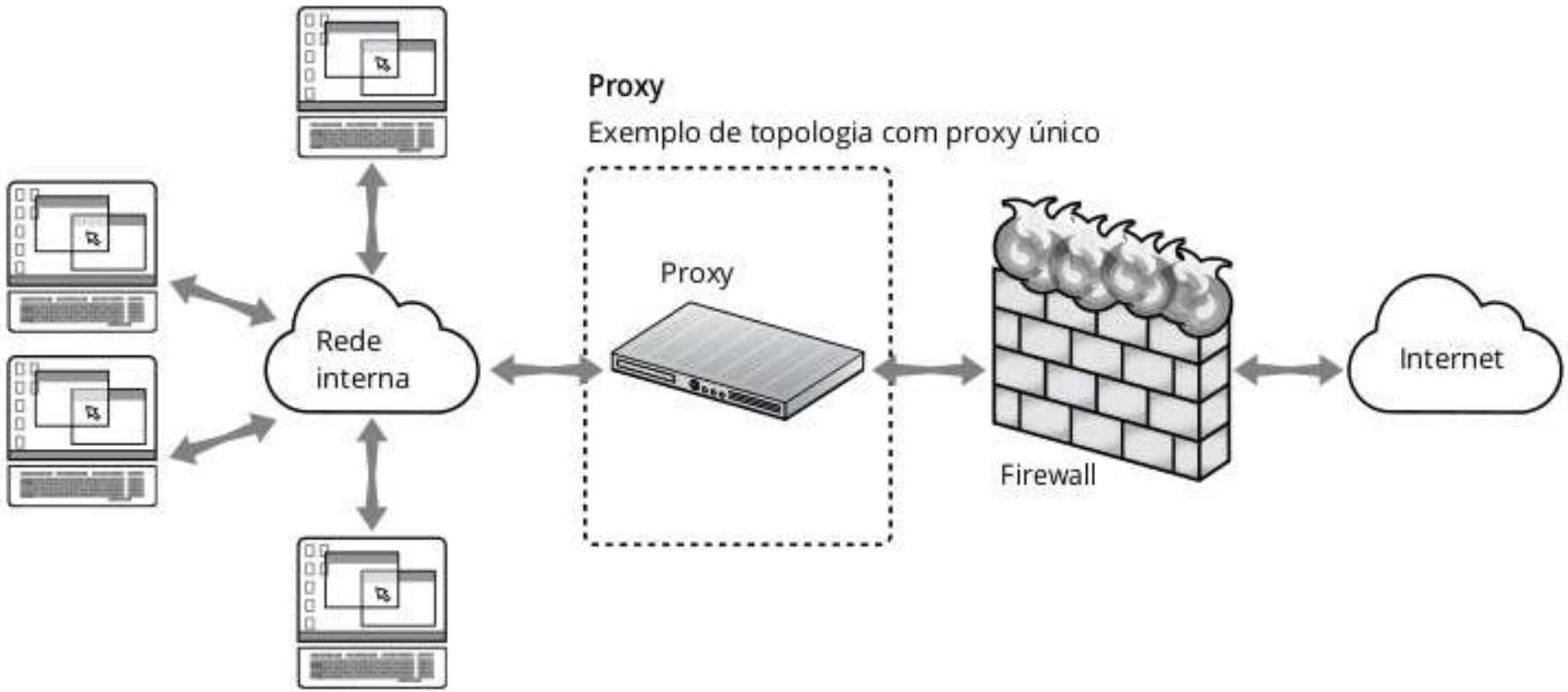
Proxy Firewall

Proxy firewall, também conhecido como firewall de aplicação ou gateway firewall, é um sistema de segurança de redes que permite análise e filtragem até a camada de aplicação.

Um proxy é um sistema de computador ou uma aplicação que age como um intermediário entre clientes e servidores, fazendo pedidos no lugar dos clientes e devolvendo respostas no lugar do servidor. O proxy firewall além disso, monitora o tráfego entre eles, a fim de proteger contra possíveis ameaças.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Proxy Firewall



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Proxy Firewall

Os proxy firewall tem um desempenho computacional inferior ao de filtro de pacote.

Proxy firewalls são considerados um dos tipos mais seguros de firewall, pois ele impede que servidores externos tenham contato direto com a rede local. Além disso, ele realiza inspeções nos protocolos da camada de aplicação, como FTP e HTTP.

Faz com que o tráfego pareça ter origem no proxy, mascarando o endereço do host interno.

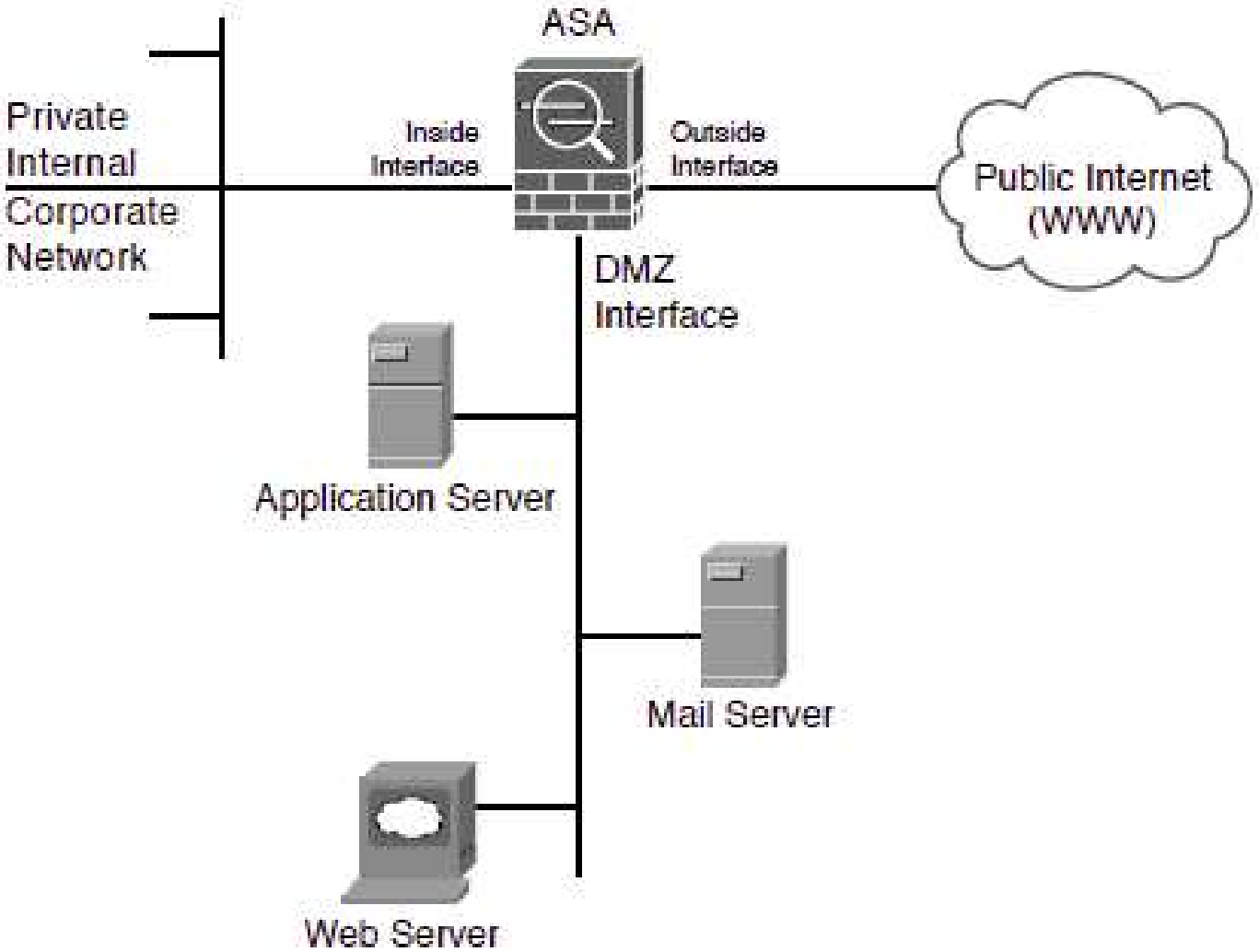
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

DMZ

DMZ é uma sigla para Demilitarized Zone (Zona Desmilitarizada), é uma subrede que se situa entre uma rede confiável (a rede local) e uma rede não confiável (internet), provendo assim isolamento físico entre as duas redes, garantido por uma série de regras de conectividade mantidas no firewall. O aspecto do isolamento físico do DMZ é importante por o mesmo garantir que a internet acesse apenas os servidores isolados no DMZ, ao invés de acessar diretamente a rede interna da sua organização. Os servidores mais comumente encontrados no DMZ são os de email, FTP, e HTML.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

DMZ



ISTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Configuração

Os passos para se configurar um firewall são:

1. Examinar a política de segurança da rede (ou seja, determinar quais endereços e aplicações podem ser acessados por quem e quando).
2. Transformar essas regras definidas em português em termos lógicos. Como um pseudo-algoritmo, por exemplo.
3. E, por fim, adequar o passo dois à sintaxe/linguagem utilizada pelo firewall em questão.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Linux

No Linux, as funções de Firewall são agregadas à própria arquitetura do kernel.

Quando uma empresa de grande porte faz a opção por uma solução de firewall baseada em software livre, não o faz pelo custo. Faz independentemente do preço. Colocamos em primeiro lugar a funcionalidade e maturidade da tecnologia. Dessa forma, soluções de firewall baseadas em Linux ou mesmo baseadas em Unix BSD são usadas por serem funcionais e confiáveis.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Exemplos

- Linux Kernel 2.0.x:
  - PF: Packet Filter.
  - IPFWADM: Packet Filter.
- Linux Kernel 2.2.x:
  - IPchains: Packet Filter.
  - Sinus: Packet Filter.
- Linux Kernel 2.4.x / 2.6.x:
  - Netfilter (Iptables): StatefulPacket.
- Outras:
  - IPFW (FreeBSD),
  - PF (OpenBSD e FreeBSD 5.x)
  - IPFilter (Solaris 10).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Iptables

O Netfilter é a parte do Kernel do Linux que vai compor as capacidades de firewall e que será configurado e gerenciado pela ferramenta chamada Iptables. Todavia, quando se menciona o firewall do Linux, é comum simplesmente denominá-lo Iptables.

Principais características

- Suporte a protocolos TCP/UDP/ICMP e IGMP, entre outros;
- Suporte a Redirecionamento de pacotes;
- É estável e rápido;
- É baseado em estados;
- Suporte a NAT

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE