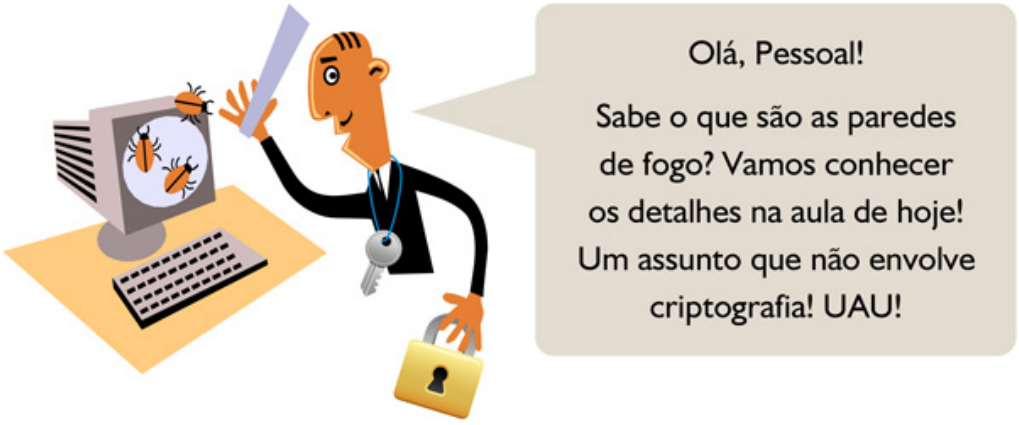
Segurança em Redes

Aula 08 - Firewall

Apresentação



Nesta aula, iremos estudar, mais detalhadamente, os firewalls, descrevendo o seu funcionamento, os tipos de firewalls, as arquiteturas, suas vantagens e desvantagens.

Vídeo 01 - Apresentação

Objetivos

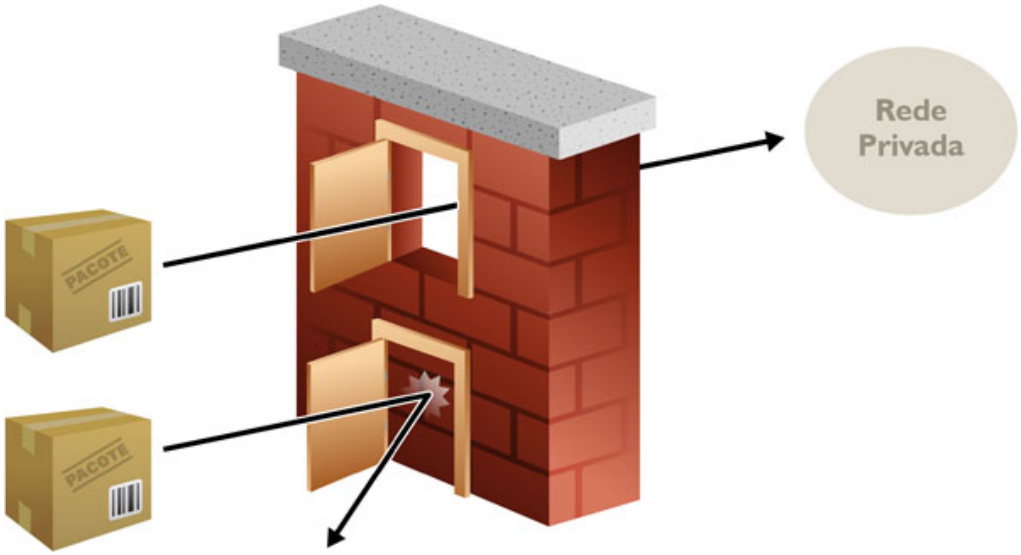
Ao final desta aula, você será capaz de:

- Saber para que servem os firewalls.
- Conhecer o funcionamento dos firewalls.
- Distinguir os tipos de firewalls.
- Distinguir as arquiteturas de firewalls.

Conceito de Firewall

Como você já viu na aula 2, firewall significa “muro ou parede corta-fogo”. Na verdade, o nome é usado para dar a ideia de uma parede que separa dois ambientes, ou melhor, duas redes de computadores. Tem como finalidade básica controlar o tráfego de pacotes entre as redes. Podemos considerar que o firewall possui “portas” através das quais os pacotes entram e saem. Essas portas possuem regras que permitem ou negam a passagem dos pacotes. A **Figura 1** mostra pacotes sendo negados e permitidos pelo firewall de uma rede privada.

Figura 01 - Pacotes selecionados por um firewall.



Finalidade do Firewall

O firewall serve como barreira de comunicação entre duas redes. Ele pode ser implementado em um roteador, computador ou hardware especificamente desenvolvido para esta funcionalidade. Independente de onde estiver implementado, será configurado para “vigiar” os pacotes que chegam ou deixam a rede interna que ele protege. Ele, normalmente, age de forma transparente para o usuário, ou seja, o usuário não tem conhecimento de que há um firewall.

O firewall define uma política de acesso à rede e obriga que todos os pacotes a ela direcionados passem por ele. Por exemplo, uma política de acesso à rede internet a partir de computadores dentro da empresa pode definir que nenhum

usuário dos computadores da empresa acesse sites de redes sociais. A política de acesso é expressa através de regras. O firewall examina os pacotes, compara com as regras e bloqueia os pacotes suspeitos e/ou não autorizados. Em suma, o firewall ajuda a impedir que:

1. A sua rede ou seu computador sejam acessados sem autorização. Dessa forma, evita-se que invasores tenham acesso às suas informações e impede-se que o funcionamento do seu sistema seja prejudicado.
2. Vírus e cavalos de troia entrem no seu computador, já que o firewall pode bloquear portas comumente usadas por esses tipos de ataques.
3. Usuários acessem sites, serviços ou sistemas não autorizados, indevidos etc.

Além disso, o firewall permite que o administrador da rede tenha controle sobre todas as ações realizadas por seus usuários. Com isso, é possível descobrir qual usuário realizou cada uma delas.

Vídeo 02 - O Que é um Firewall?

Atividade 01

1. Liste problemas de segurança que podemos ter em uma rede que não utiliza firewall.

Regras de Filtragem

As regras de filtragem são listas de acesso que definem os tipos de acesso permitidos ou não em uma rede. A **Figura 2** ilustra os componentes básicos encontrados em uma regra de firewall.

#regra	ação	protocolo	origem	destino	opções

Figura 2 - Componentes de uma regra.

O primeiro campo é um identificador da regra. O segundo campo estabelece se a ação é permitir ou negar a passagem do pacote. O terceiro campo refere-se ao protocolo (normalmente de rede, transporte ou aplicação), utilizado pelo pacote. O quarto campo indica a origem do pacote. O quinto campo indica o seu destino. O sexto campo define, por exemplo, os flags do pacote e portas de origem ou destino. A seguir, veremos alguns exemplos de regras.

Exemplo 1

Se o administrador deseja impedir conexões do serviço telnet para sua rede interna (protocolo TCP, porta 23), deve configurar uma regra de firewall conforme mostra a **Figura 3**.

#regra	ação	protocolo	origem	destino	opções
01	negar	TCP	qualquer	Rede interna	Porta destino = 23

Figura 3 - Exemplo de regra para impedir telnet.

Exemplo 2

Se o administrador desejar abrir uma exceção, permitindo conexões telnet vindas de um determinado local, então adiciona-se uma nova regra que contenha o endereço de origem deste local, por exemplo, 1.2.3.4. As regras na **Figura 4** mostram que todos os pacotes para a porta 23 serão bloqueados, exceto os que possuem como origem o endereço 1.2.3.4.

#regra	ação	protocolo	Origem	destino	opções
01	permitir	TCP	1.2.3.4	Rede interna	Porta destino = 23
02	negar	TCP	qualquer	Rede interna	Porta destino = 23

Figura 4 - Exemplo de regras para telnet

Exemplo 3

Com isso, você pode pensar que vamos precisar criar uma regra nova para cada restrição ou liberação. Mas, isso não é verdade. Se duas restrições não se excluírem, elas podem vir a fazer parte da mesma regra.

Uma questão importante refere-se à prioridade das regras, que influencia diretamente a política de segurança da rede. Uma opção seria liberar tudo e estabelecer regras específicas de negação. Outra opção seria negar tudo e liberar o que for necessário. Certamente, a segunda opção é mais segura, mas a manutenção será mais trabalhosa, pois a cada novo serviço que surgir, o administrador terá que incluir uma nova regra para liberá-lo.

Adotando a primeira opção (liberar tudo e ter regras de negação), suponha que queremos bloquear o acesso a serviços que estão em portas menores que 1024, que são serviços que precisam ser executados com privilégios de root. A **Figura 5** ilustra essa regra.

#regra	ação	protocolo	origem	destino	opções
01	negar	TCP/UDP	qualquer	Rede interna	Porta destino < 1024

Figura 5 - Exemplo de regra para impedir portas inferiores a 1024

Exemplo 4

Conforme visto, o campo “opções” poderá conter uma série de informações além da porta de origem ou destino. Por exemplo, é bastante comum termos regras onde se leva em consideração informações do “estado” de uma conexão TCP (contidas no cabeçalho de seus frames). Com isso, conforme visto na **Figura 6**, podemos bloquear apenas novas tentativas de conexão a um serviço, sem influir nas já estabelecidas.

#regra	ação	protocolo	origem	destino	opções
01	Negar	TCP	qualquer	Rede interna	Porta destino = 80 Estado = new

Figura 6 - Exemplo de regra que usa o flags do TCP

Atividade 02

1. Escreva uma regra que impeça acessos ao serviço de correio eletrônico (TCP/25), vindos do endereço IP 5.6.7.8.

Tipos de Firewall

Existem diferentes tipos de firewall, que se distinguem pela forma como operam.

Nesta seção, vamos conhecer alguns tipos bem conhecidos de firewall e seus modos de operação.

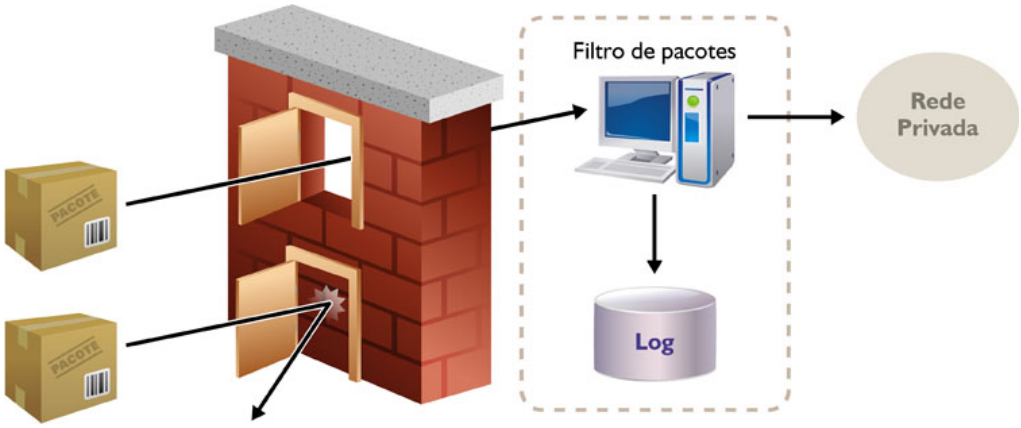
Filtros de Pacotes

Podem ser implementados de diversas formas, como em switchs, roteadores, computadores com sistema operacional apropriado ou hardware de propósito específico (normalmente comercialmente chamados de *appliance*). Seja qual for o caso, o equipamento deverá estar ligado à rede externa (comumente a internet) e à rede interna. O tráfego entre as redes se dá (ou não) conforme as regras estabelecidas. Esse é o tipo de firewall mais antigo, sendo atualmente considerado simples, e possuindo um pequeno conjunto de funcionalidades. Devido a seu funcionamento interno ser bastante simples, o uso desse tipo de firewall normalmente irá implicar na necessidade de um maior número de regras de filtragem (quando comparado a outros tipos). Outra desvantagem, que parece um

contrassenso, é que, apesar de sua simplicidade interna, esse tipo de firewall é o que exige maiores quantidades de memória e processamento para seu funcionamento.

Em todos os tipos de firewall que serão estudados, uma funcionalidade importante é a possibilidade de registrar (ou logar) informações referentes ao seu funcionamento. Normalmente, essa funcionalidade é utilizada para se documentar as tentativas de acesso não autorizadas, que tentaram passar pelo firewall. Com base nessas informações, podemos, por exemplo, identificar possíveis atacantes, ou até mesmo definir ações a serem tomadas na ocorrência de algum evento em especial relacionado à segurança. A **Figura 7** ilustra um filtro de pacotes.

Figura 07 - Filtro de pacotes.



Filtros de Pacotes com Estados

Os filtros de pacotes com estados surgiram para sanar as desvantagens existentes nos filtros de pacotes “tradicionais”. Seu funcionamento interno é bem mais complexo, por isso, normalmente, só são encontrados em computadores com sistema operacional apropriado ou hardware de propósito específico. Uma das vantagens desse tipo de firewall já foi vista nesta aula: a possibilidade de se criar regras mais especializadas, que levam em conta, por exemplo, os flags de estado do protocolo TCP.

Contudo, sua principal vantagem está no fato de que, apesar de ter um funcionamento interno mais complexo, eles exigem bem menos memória e processamento que os filtros de pacotes “tradicionais”. Isso ocorre porque em um filtro tradicional todos os pacotes que pertencem, por exemplo, a uma mesma conexão TCP serão, obrigatoriamente, analisados pelas regras de filtragem. Em um

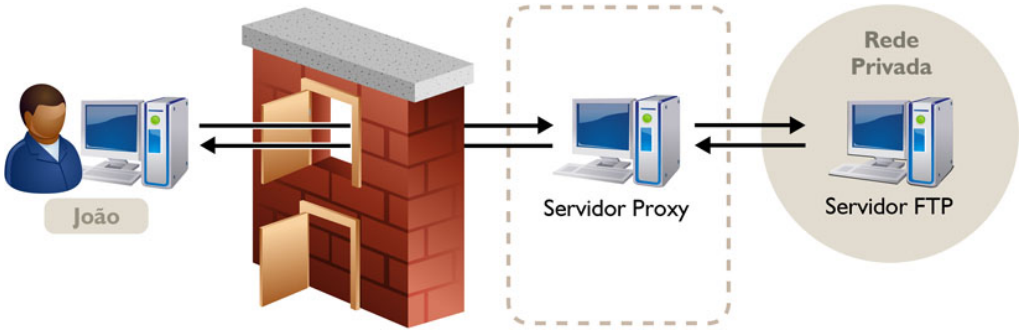
filtro com estados, isso não é necessário. Neles, apenas os pacotes de abertura de conexão precisam ser realmente analisados pelo conjunto de regras de filtragem. Caso a conexão seja permitida, essa informação será inserida na base de estados como uma conexão autorizada. Todos os pacotes subsequentes, pertencentes a essa mesma conexão, serão "automaticamente" autorizados, sem que seja necessário percorrer as regras novamente. Um firewall que armazena informações de estado pode ser visualizado na **Figura 8**.

Figura 08 - Filtro de pacotes com estados.

Servidores Proxy

Servidores proxy atuam como intermediários na comunicação entre clientes e servidores de um serviço. Eles recebem as requisições de um ou mais clientes e as repassam para os servidores de destino. Opcionalmente, um servidor proxy pode implementar uma série de outras funcionalidades, tais como a filtragem das requisições realizadas pelos clientes. Isso faz com que os servidores proxy sejam considerados um tipo de firewall que funciona a nível de aplicação. A **Figura 9** mostra um modelo genérico de uso dos servidores proxy. Vale salientar que os servidores proxy não irão definir novos protocolo de aplicação, mas sim utilizar as funcionalidades dos já existentes, como HTTP e FTP.

Figura 09 - Servidor Proxy.



Quando utilizados, como visto na **Figura 9**, os servidores proxy também podem ser responsáveis por permitir que os clientes da rede interna acessem um serviço ou conjunto deles na Internet. Dessa forma, se o servidor proxy dessa figura implementa os protocolos HTTP e FTP, esses serão os únicos serviços da Internet acessíveis para os clientes da rede interna.

Vídeo 03 - Tipos de Firewall

Atividade 03

1. Quais as principais desvantagens dos filtros de pacotes tradicionais?

Arquiteturas de Firewall

A arquitetura (posicionamento e funções realizadas) de um firewall deve ser definida conforme as necessidades da instituição.

Vamos mostrar as principais arquiteturas e suas características.

Roteador ou Filtro de Pacotes com Filtragem

Essa é a arquitetura mais simples. Nela, a filtragem de pacotes é realizada no próprio roteador ou máquina com software de firewall instalado, conforme ilustra a **Figura 10**. A arquitetura é transparente para as partes envolvidas: os computadores da rede interna podem se comunicar diretamente com a internet.

Figura 10 - Roteador com filtragem.

Gateway de Aplicação (proxy)

Esta arquitetura é normalmente utilizada pelos servidores proxy, estudados anteriormente. Nela, o proxy deve possuir duas interfaces de rede, isolando-as, conforme ilustra a **Figura 11**.

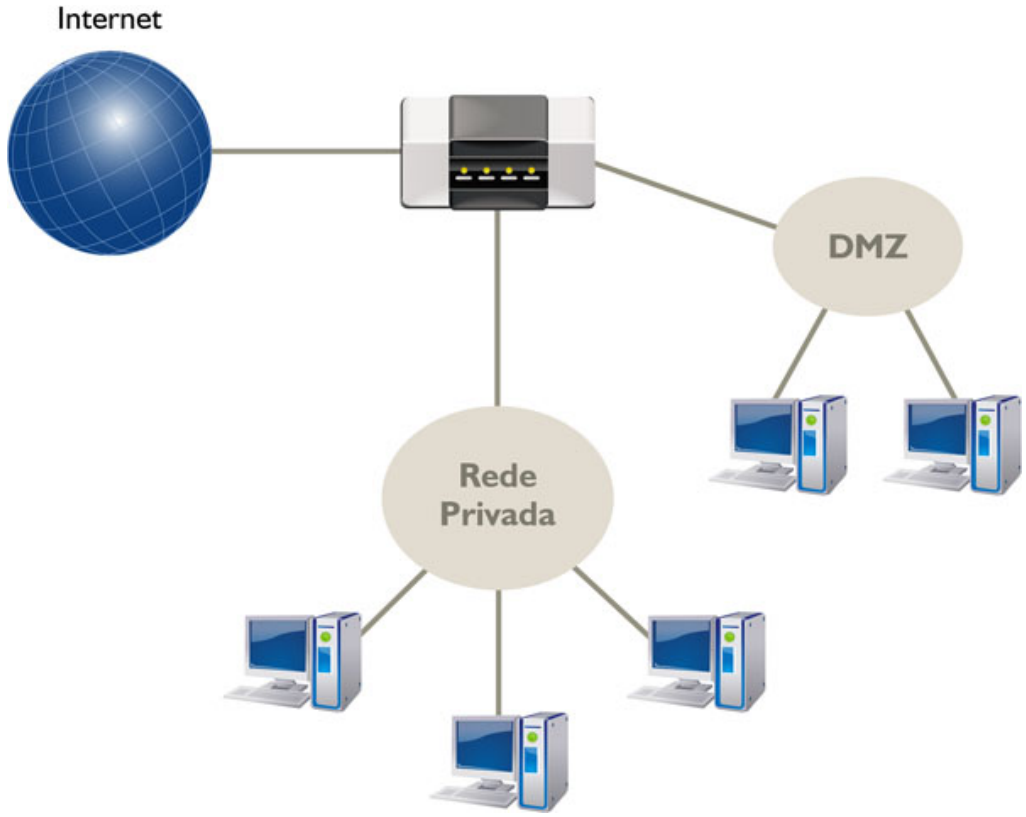
Figura 11 - Gateway de aplicação (proxy).

Nesse caso, para exercer a função de firewall, o roteamento é desativado. Isso significa que os pacotes da rede privada não são encaminhados diretamente à internet ou vice-versa, todo o repasse é realizado pelo serviço de proxy.

Rede Interna com DMZ

A arquitetura de rede com DMZ adiciona uma nova rede de perímetro para isolar mais ainda a rede interna da internet, conforme ilustra a **Figura 12**. Uma DMZ — demilitarized zone, ou zona desmilitarizada, é uma rede onde concentramos todos os computadores para os quais é permitido algum tipo de acesso externo. Nessa arquitetura, o firewall irá permitir os acessos autorizados no sentido internet → DMZ, e negar qualquer tipo de acesso no sentido internet → rede interna. Serão autorizados apenas acessos no sentido rede interna → internet.

Figura 12 - Rede interna com DMZ.



Atividade 04

---

1. Compare as arquiteturas de firewall que você estudou.
2. Qual a vantagem de sua rede possuir uma DMZ?

Princípios Básicos de um Projeto de Firewall

Ao implantar o firewall de uma rede, devemos seguir alguns princípios básicos, essenciais para que o firewall realmente forneça uma boa proteção. Os seguintes princípios devem ser observados.

a. **Atenção aos modos de falha**

- Se houver algum problema com o firewall (máquina falhar, travar...), a atitude padrão é impedir a passagem de todo o tráfego.

b. **Use listas de verificação que identificam se:**

- O firewall reflete a política da empresa;
- Filtros de pacotes usam conjunto de regras simples;
- Serviços disponíveis para acesso externo estão configurados de forma segura, etc.

c. **Use ferramentas de verificação que monitorem o tráfego que passa pelo firewall.**

Vantagens e Desvantagens

O firewall é uma forma de proteção muito importante, mas ele tem vantagens e desvantagens:

As vantagens do firewall:

- Oferece um único ponto de acesso à rede, concentrando o gerenciamento da segurança e a localização de problemas;
- Somente tráfego autorizado (definido pela política de segurança da rede) é autorizado a passar.

As desvantagens do firewall:

- É um ponto de falha centralizado;
- A violação do firewall faz com que toda a rede fique vulnerável.

Vamos pensar em algumas coisas que aprendemos até hoje e identificar algumas funções de segurança que o firewall não realiza? Por exemplo, o firewall não garante autenticidade da origem de um pacote ou sua integridade. Ele não controla como os pacotes foram criados, nem quem os criou.

Um Exemplo de Firewall: IPTables

O IPTables é um comando disponível na maioria das distribuições Linux que comunica-se com uma biblioteca existente no kernel desse sistema operacional, chamada de NetFilter. Ele é o firewall padrão do Linux, compreendendo os conceitos que aparecem a seguir.

Regras: são comandos passados ao Netfilter para realizar uma determinada ação de acordo com, por exemplo, o endereço/porta de origem/destino, interface de origem/destino etc. O NetFilter realiza a comparação dessas regras com os pacotes que passam pela rede para autorizá-los ou não.

Chains: as regras são armazenadas em chains, que podem ser de dois tipos: os padrões (Ex: *INPUT*, *OUTPUT* e *FORWARD*) e os criados pelo usuário.

Tabelas: são locais usados para armazenar os chains e regras com características semelhantes. Existem três tabelas disponíveis no NetFilter, que são FILTER, NAT e MANGLE. Na tabela FILTER, são definidos quais pacotes podem passar ou não. Isso é justamente um filtro de pacotes. A tabela NAT (*Network address translation*) refere-se aos pacotes que vão sofrer tradução de endereço. A tabela MANGLE define quais pacotes serão marcados para uma ação posterior.

Alvo: é a ação a ser tomada quando um pacote “casa” com uma regra existente em uma chain. No IPTables, existe, entre outros: ACCEPT, DROP, REJECT e QUEUE. O ACCEPT permite que pacote chegue ao seu destino. A ação DROP nega o pacote sem

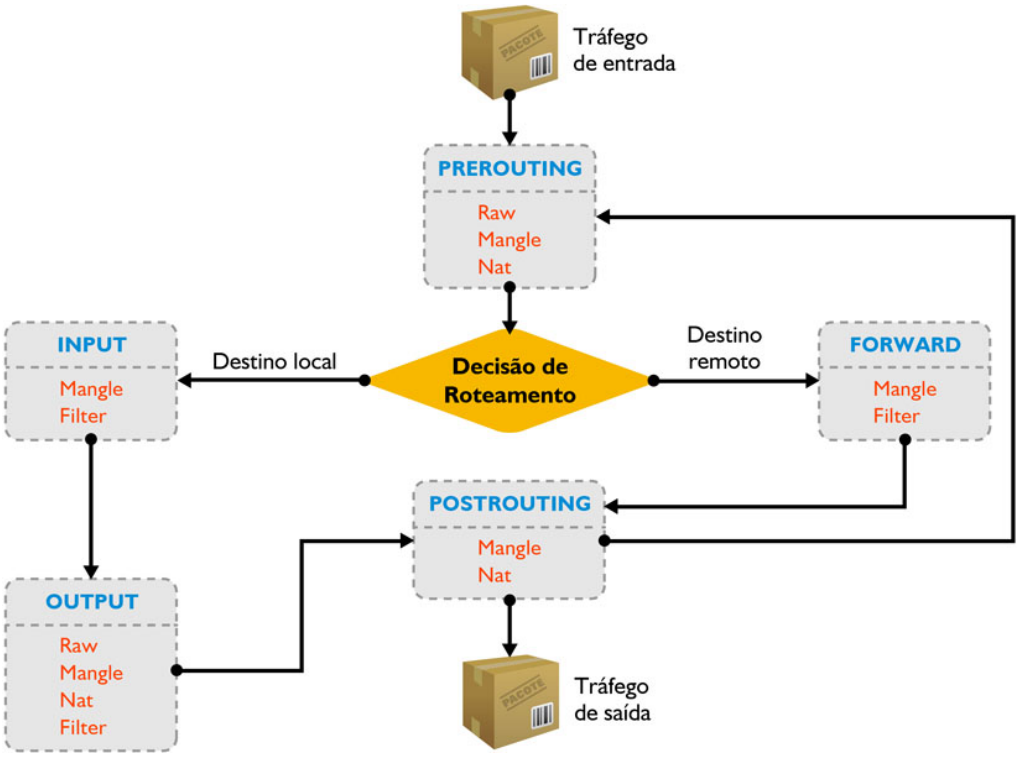
retornar mensagem. A ação REJECT, por sua vez, nega a passagem do pacote, retornando uma mensagem. Por fim, o QUEUE envia pacote ao espaço do usuário.

O IPTables tem vários comandos para manipular as chains. Por exemplo, -L [Chain] lista as regras de uma chain. Esse curso tem como finalidade dar uma visão geral sobre os firewalls, por isso estamos citando o IPTables apenas para ilustrar. Não vamos, portanto, detalhar a vasta lista de comandos por ele disponibilizados. Um exemplo de uso do IPTables é a linha de código mostrada a seguir.

```
1 iptables –t filter –A INPUT –d 7.8.9.10 –j DROP
```

Nela, usamos o IPTables para incluir uma regra "A" no chain INPUT (*-A INPUT*) que bloqueia (*-j DROP*) qualquer acesso destinado ao endereço 7.8.9.10 (-d 192.168.0.1).

Figura 13 - Fluxo de pacotes e processamento no NetFilter.



Fonte: http://danielmiessler.com/study/iptables/ Acesso em: 29 ago. 2012

Vídeo 04 - Tipos de Firewall

A **Figura 13** mostra como ocorre o fluxo de dados internamente no kernel do Linux. Os pacotes movem-se atravessando as chains. Em cada quadrado da figura, são mostrados os chains do NetFilter (em azul) e as tabelas válidas para aquele chain (em vermelho). Por exemplo, na chain INPUT, existem as tabelas Mangle e Filter. Os pacotes que se enquadram nesta chain irão passar sequencialmente por elas. Se o pacote casa com alguma regra dessas tabelas, ele é processado. Se o pacote não casa com as regras, ele pode ser aceito ou descartado — isso depende da política implementada. Se a política for descartar todos os pacotes que não casam com nenhuma regra (a mais comum), ele será descartado.

Vídeo 05 - Netfilter e Squid

Atividade 05

1. Quais as possíveis ações que podem ser tomadas quando um pacote é tratado pelo IPtables?

Atividade 06

Pesquisa

1. Pesquise alguns exemplos de firewalls utilizados no Windows.

Leitura Complementar

- Revisão geral sobre firewall. Acesse: http://www.abandonemicrosoft.net/publico/Textos e Documentos/Seminario Firewall.pdf. Acesso em: 29 ago. 2012.

- Firewall: Principais considerações do CSO: http://segurancadainformacao.modulo.com.br/firewall-principais-consideracoes-do-cso

- Boas práticas na administração de seu firewall de rede: https://www.blockbit.com/pt-br/2017/07/17/boas-praticas-na-administracao-de-seu-firewall-de-rede/

Resumo

Na aula de hoje, você aprendeu que o firewall é o primeiro elemento de defesa de uma rede. Ele deve estabelecer regras que, quando implementadas, estejam de acordo com a política de segurança da organização, definindo os serviços permitidos e proibidos. Basicamente, um firewall define que “tudo o que não for explicitamente negado é permitido” ou “o que não for explicitamente permitido é negado”. Os tipos de firewall que você estudou foram: filtros de pacotes; filtros com estados e servidores proxy. As arquiteturas de firewall que você viu nesta aula foram: Roteador ou filtro de pacotes com filtragem; Gateway de aplicação (proxy) e Rede interna com DMZ. Nesta aula, você também estudou os princípios básicos de um projeto de firewall, as suas vantagens e desvantagens, e conheceu um exemplo de firewall chamado IPTables.

Autoavaliação

1. Cite as desvantagens dos filtros de pacotes tradicionais.

2. Explique por que os servidores Proxy são considerados um tipo de firewall.

3. Marque V ou F (V para verdadeiro e F para falso):

   ( ) Firewalls com estado são os que possuem o menor conjunto de funcionalidades.
   ( ) A DMZ concentra os computadores para os quais é permitido algum tipo de acesso externo.
   ( ) Filtros de pacotes tradicionais são comuns em roteadores.
   ( ) Uma única regra de firewall pode bloquear o acesso a diversas portas TCP e UDP da rede interna.

Referências

GUIA Foca GNU/Linux. Disponível em: <http://www.guiafoca.org/?page_id=14>. Acesso em: 15 out. 2012.

NAKAMURA, E; GEUS, P. L. **Segurança em Redes em Ambientes Cooperativos**. Rio de Janeiro: Novatec, 2007.

ORNELLAS, Fabio Pugliese. **Firewall e roteamento avançado no Linux**. Disponível em: <segurancadainformacao.modulo.com.br/firewall-principais-consideracoes-do-cso>. Acesso em: 29 ago. 2012.