SEGURANÇA DE REDES DE COMPUTADORES

SOLUÇÕES EDUCACIONAIS INTEGRADAS

Introdução a *firewall*

Juliane Adelia Soares

OBJETIVOS DE APRENDIZAGEM

- Descrever as funcionalidades de um *firewall*.
- Diferenciar os filtros de pacotes e filtros de pacote com estados.
- Explicar o funcionamento dos servidores *proxy*.

Introdução

Na Era Digital, a tecnologia impera em praticamente todos os processos organizacionais. Embora contar com tanta tecnologia seja extremamente vantajoso, as informações ficam muito expostas a um crescente e variável número de riscos por consequência desse ambiente cada vez mais interconectado. Portanto, a segurança de redes de computadores tornou-se fundamental no mundo corporativo.

É impossível não destacar que as informações, não apenas na Era Digital, mas desde os primórdios, são o ativo mais importante dentro das organizações, de modo que é de extrema importância protegê-las não apenas quando armazenadas, mas também durante sua transmissão. Isso é possível com a adoção da segurança da informação, que faz uso de *softwares* e *hardwares* para uma proteção mais efetiva. Nesse contexto, o *firewall* é um importante dispositivo de segurança de redes.

Neste capítulo, vamos descrever esse dispositivo, destacando suas principais funcionalidades. Vamos, ainda, destacar as diferenças entre os filtros de pacotes e os filtros de pacotes com estados, e explicar como funcionam os servidores *proxy*.

Firewall: funcionalidades

Redes de computadores são redes distribuídas e fortemente conectadas (quando compartilham inúmeros recursos de um computador central) ou fracamente conectadas (quando compartilham apenas recursos necessários para o funcionamento da rede). A segurança de redes de computadores envolve a criação de um ambiente de proteção, que contempla todos os recursos de uma rede, todos os dados nela armazenados e em trânsito e todos seus usuários (KIZZA, 2020).

Obviamente, os recursos precisam ser protegidos de acessos não autorizados internos e externos. Esses recursos, sejam eles físicos ou não, são objetos, que podem ser tangíveis ou intangíveis. Nas redes de computadores, os **objetos tangíveis** são os recursos de *hardware* e os **objetos intangíveis** são os dados dos sistemas, tantos os estáticos, no armazenamento, quanto os que estão em transição.

As **proteções de *hardware*** consistem em proteger objetos de usuário final, incluindo componentes de *hardware* de interface do usuário, como componentes de entrada. Objetos de rede como *firewalls*, *hubs*, *switches*, roteadores e *gateways* devem ser protegidos, bem como os canais de comunicação de rede, de modo que esta não seja interceptada.

Já as **proteções de *software*** consistem em proteger os recursos de *software* e incluem a proteção de *software* baseado em *hardware*, de sistemas operacionais, de protocolos de servidores, de navegadores e de *softwares* de aplicação, além da proteção de propriedade intelectual armazenada em discos de armazenamento de rede e bancos de dados. A proteção de *software* também envolve a proteção do *software*-cliente.

Para que a segurança de redes seja eficiente, ela envolve uma série de componentes que devem trabalhar em conjunto, como *softwares* contra *malwares*, sistemas de detecção e prevenção de intrusão (IDS, do inglês *intrusion detection system*, e IPS, de *intrusion prevention system*) e *firewalls*. Neste capítulo, nosso foco será o *firewall*.

O ***firewall*** é uma técnica de rede muito efetiva. Seu nome vem de portas corta-fogo (*firewalls*), que são muito utilizadas em edifícios, por exemplo, para conter o fogo de possíveis incêndios, evitando que se espalhe para o restante do prédio. É basicamente isso que um *firewall* faz em uma rede (Figura 1), já que nem todo tráfego é autorizado (PEIXINHO; FONSECA; LIMA, 2013).

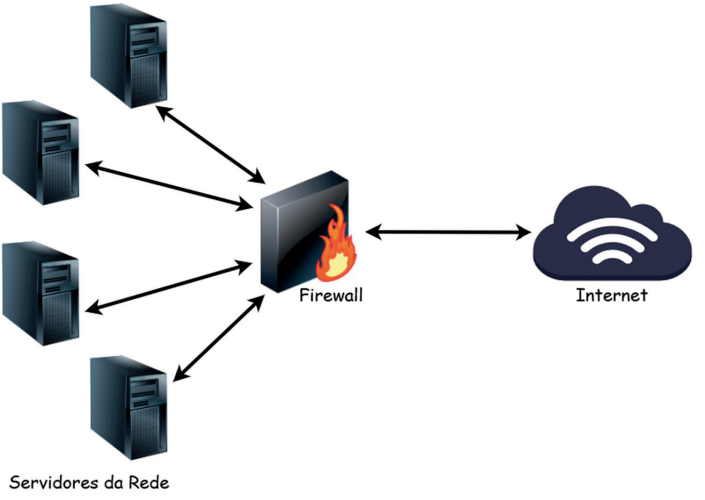

Figura 1. Posicionamento do *firewall*.

O *firewall* é um dispositivo de *hardware* ou uma solução de *software* responsável por impedir acessos não autorizados a uma rede. Ele realiza a inspeção de todo o tráfego de entrada e de saída pelo uso de um conjunto de regras, de modo a identificar e bloquear ameaças. *Firewalls* são utilizados em configurações tanto pessoais quanto empresariais, vindo como parte integrante em muitos dispositivos, incluindo computadores MAC, Windows e Linux, e são considerados componentes essenciais para a segurança de rede (LUTKEVICH, 2021).

Como mostrado na Figura 1, o *firewall* é inserido entre a rede e a internet para que seja estabelecida uma ligação controlada, montando um perímetro de segurança externo, cuja meta é a proteção da rede contra ataques provenientes da internet, provendo um ponto único de estrangulamento, em que segurança e auditoria possam ser impostas. Dessa forma, ele provê uma camada de defesa adicional, mantendo os sistemas internos isolados das redes externas. O *firewall* pode ser um sistema de computador separado, um serviço de *software* em execução em um roteador ou servidor existente, bem como uma rede separada, contendo diversos dispositivos de suporte (STALLINGS; BROWN, 2014).

Fique atento

Algumas empresas optam por adicionar *firewalls* com diferentes níveis de confiança entre partes do ambiente de rede, visando a garantir proteção extra para aplicações e dados mais importantes.

Stallings e Brown (2014) citam as principais metas de um projeto de *firewall*, listadas a seguir.

- Todo o acesso à rede local deve ser bloqueado fisicamente, sendo possível realizá-lo apenas via *firewall*. Dessa forma, o tráfego como um todo, o de dentro para fora e o de fora para dentro, passará inteiramente pelo *firewall*.
- O tráfego permitido deve ser definido pela política de segurança local. Assim, somente o tráfego autorizado terá permissão para passar pelo *firewall*.

Stallings e Brown (2014) também listam as seguintes quatro técnicas gerais utilizadas pelos *firewalls* para controlar o acesso e impor a política de segurança.

1. **Controle de serviço:** é responsável por determinar os tipos de serviço da internet que poderão ser acessados de dentro para fora e de fora para dentro de uma rede. Portanto, o *firewall* realiza a filtragem do tráfego baseado no endereço IP (*internet protocol*), no protocolo ou no número de porta. É possível, para o *firewall*, prover *software proxy*, recebendo e interpretando cada requisição de serviço antes que ela siga até o destino. Também, é possível que o próprio *software*-servidor seja hospedado como serviço *web* ou de correio.
2. **Controle de direção:** é responsável por determinar a direção em que determinadas requisições de serviço podem ser iniciadas e têm permissão de transitar pelo *firewall*.

3. **Controle de usuário:** o acesso aos serviços é controlado de acordo com o usuário que deseja acessá-lo e é um recurso aplicado a usuários locais, ou seja, localizados dentro do perímetro do *firewall*. Porém, também pode ser aplicado a tráfego de entrada, originado de usuários externos. Para isso, é necessária uma forma de tecnologia de autenticação segura, como o protocolo IPSec (*internet protocol security*), que é um conjunto de protocolos responsável por proteger as comunicações de rede na camada IP, facilitando uma autenticação bidirecional entre os dispositivos de rede que trocam dados pela utilização de chaves para autorizar os pacotes de dados.
4. **Controle de comportamento:** todo o modo de utilização de determinados serviços é controlado, como, por exemplo, liberar apenas algumas partes das informações de servidores na rede para acessos externos.

Por terem gerenciamento baseado em regras, os *firewalls* gerenciam a segurança de redes definindo regras sobre o que é aceitável ou não. Essas regras são filtros configurados no *firewall* facilitando a implementação de inúmeros requisitos de segurança. Os recursos de filtragem também impõem divisões entre as redes, a fim de evitar que o tráfego se mova de uma rede a outra. Além disso, os *firewalls* utilizam as regras para a proteção contra inundação, ou seja, podem ser configuradas regras para limitar largura de banda do tráfego dos *hosts*, o que reduz a capacidade de um *host* inundar a rede. Outra funcionalidade do *firewall* é a proteção de *loop*. Isso significa que eles podem examinar os endereços das mensagens, de modo que seja possível determinar se alguma mensagem está sendo enviada em *loop* interminável (o que também é uma forma de inundação) (KIM; SOLOMON, 2018).

O *firewall* tem um único ponto de estrangulamento definido, com a finalidade de manter usuários não autorizados fora da rede que está sendo protegida. Além do mais, proíbe que serviços potencialmente vulneráveis entrem ou saiam da rede, provendo proteção contra diferentes tipos de falsificação de IP e ataques de roteamento. Isso facilita muito a proteção, pois as funcionalidades de segurança ficam concentradas em um único sistema ou conjunto de sistemas. O *firewall* fornece um local onde é possível monitorar ocorrências relacionadas à segurança, e auditorias e alarmes podem ser implementados no sistema do *firewall* (STALLINGS; BROWN, 2014).

Além disso, um *firewall* tem funcionalidades que não se relacionam com a segurança, como o tradutor de endereços de rede, que é responsável por mapear endereços locais, para endereços de internet, ou então gerenciar redes, fazendo auditoria ou registrando a utilização da internet.

Apesar de suas funcionalidades, os firewalls também apresentam limitações, que são citadas por Stallings e Brown (2014) e a seguir listadas.

- Alguns sistemas internos podem ter recursos de discagem ou de banda larga móvel para se conectar a um provedor de serviços, assim como uma LAN (*local area network*) interna pode ter suporte a recursos do *modem* que fornecem a capacidade de acesso discado na rede para colaboradores que viajam ou trabalham de casa. Dessa forma, o *firewall* não seria uma proteção eficiente, já que não é possível proteger o que não passa por ele.
- Em alguns casos, a ameaça se encontra dentro da própria empresa, como um funcionário insatisfeito, por exemplo, que pode cooperar com um atacante externo, o que o *firewall* dificilmente consegue proteger.
- Os ataques podem vir por meio de dispositivos de armazenamento portátil, como um *pen-drive*. Esses dispositivos são utilizados em equipamentos fora da rede, de modo que podem, então, ser utilizados e infectados fora da rede e, após, ser conectados a um dispositivo dentro da rede. É aí que entra o primeiro item: o *firewall* não vai proteger contra ataques que não passam por ele.

Conhecendo todas as funcionalidades de um *firewall* e suas limitações, é necessário a busca pela ferramenta que mais se encaixa nas necessidades de proteção do negócio. Essa decisão, é claro, também depende muito do investimento financeiro que a organização está disposta a fazer. Existem diversas soluções comerciais de *firewall* no mercado. A Forrester Wave (HOLMES *et al.*, 2020) fez uma avaliação dos principais fornecedores de *firewall* corporativo no terceiro trimestre de 2020 (Figura 2).

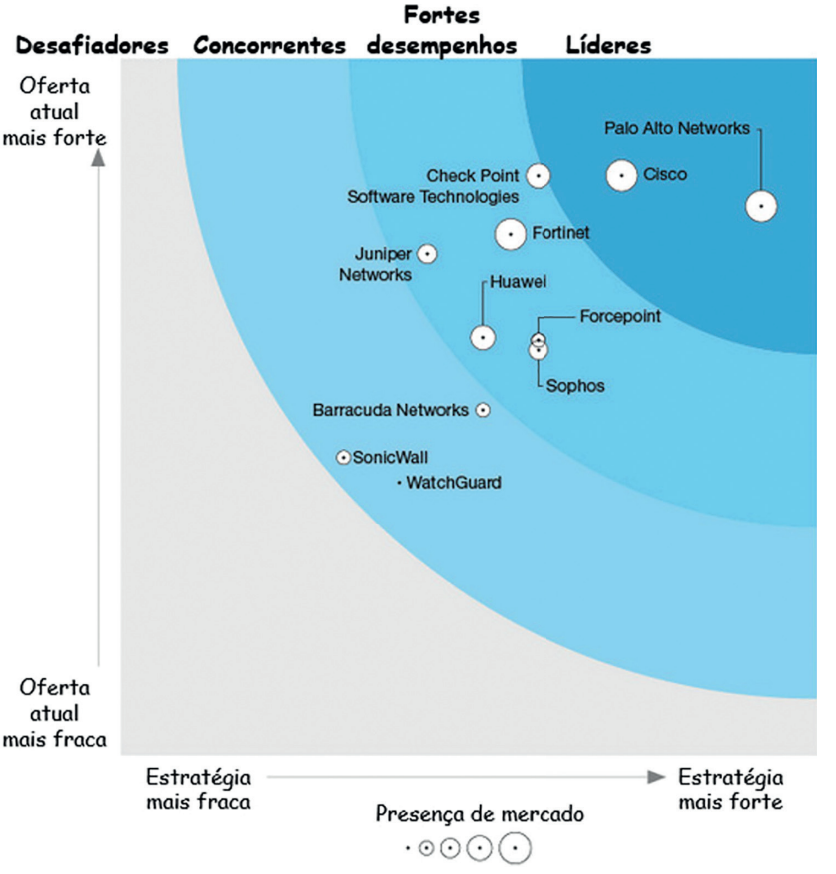

Figura 2. *Firewalls* corporativos.
Fonte: Holmes *et al.* (2020, documento *on-line*).

A avaliação apresentada na Figura 2 engloba pontos como ofertas mais fortes e mais fracas, estratégias mais fortes e mais fracas, presença de mercado e fabricantes desafiadores, competidores, que apresentam bons desempenhos, e os líderes de mercado. É possível observar que os líderes de mercado são Cisco e Palo Alto Networks, tendo pouca diferença em relação aos outros quesitos de mercado avaliados entre os dois fabricantes. Enquanto isso, Check Point Software Technologies, Fortinet, Forcepoint, Sophos, Juniper Networks e Huawei oferecem bom desempenho, e Barracuda Networks, WatchGuard e SonicWall são concorrentes.

Na próxima seção, vamos tratar dos tipos de *firewall*.

Tipo de *firewall*

Os *firewalls* podem ser classificados de acordo com o que são e onde se localizam. Eles podem ser de *hardware*, de *software* ou baseados em nuvem. O ***firewall* de *software*** se localiza em um *endpoint*, como um computador ou dispositivo móvel, e controla o tráfego diretamente no dispositivo em que está instalado. Já o ***firewall* de *hardware*** é um equipamento físico, inserido entre o *gateway* e a rede, controlando o tráfego da rede como um todo. Já os **baseados em nuvem** realizam seu trabalho a partir da nuvem, assim como qualquer outra solução SaaS (*software as a service*) (STONE, 2020).

No entanto, os *firewalls* também podem ser classificados de acordo com sua funcionalidade, dependendo de seus recursos e do nível de segurança que oferecem. Stallings e Brown (2014) definem dois tipos: filtros de pacotes e filtros de pacote com estados. Vejamos cada um em detalhes a seguir.

Firewall de filtro de pacotes

O *firewall* de filtragem de pacotes é uma das mais antigas e simples tecnologias de *firewall*. Ele faz a análise do conteúdo de cada pacote no tráfego de forma individual, utilizando, como base, os endereços de IP, o número da porta e o protocolo em uso. Observe a Figura 3.

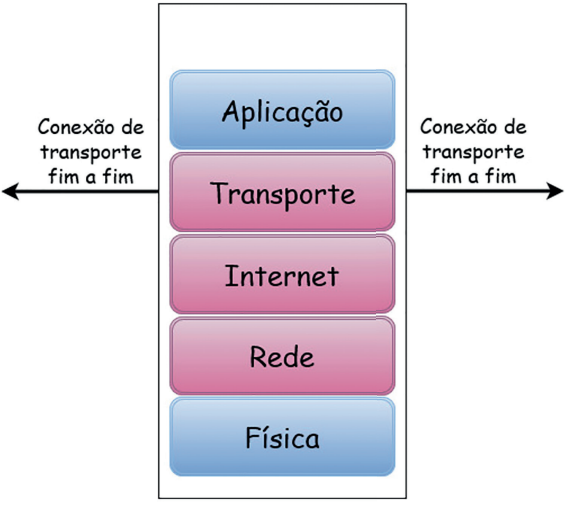

Figura 3. *Firewall* de filtragem de pacotes.
Fonte: Adaptada de Stallings e Brown (2014).

A Figura 3 mostra as camadas do modelo TCP/IP em que o *firewall* de filtragem de pacotes atua: camada de transporte (TCP, do inglês *transmission control protocol*, ou UDP, de *user datagram protocol*), camada de internet (IP) e camada de rede (ethernet). Esse tipo de *firewall* é configurado de modo que sejam filtrados os pacotes que transitam em ambas as direções, ou seja, da rede externa para a interna e da interna para a externa, definindo se o pacote é transmitido ou descartado. A filtragem ocorre de acordo com as regras definidas pelos administradores de rede. A base dessas regras de filtragem são informações contidas em pacote de rede, como as listadas a seguir.

- Endereço IP de origem: endereço IP do sistema de origem do pacote.
- Endereço IP de destino: endereço IP do sistema que o pacote está tentando alcançar.
- Endereços de origem e de destino no nível de transporte: número da porta em nível de transporte no modelo TCP/IP, utilizando protocolos como TCP ou UDP para definir aplicações como SNMP (*simple network management protocol*).
- Campo IP de protocolo: responsável por definir o protocolo de transporte.
- Interface: refere-se à interface do *firewall* de origem do pacote ou à interface de destino, quando se trata de um *firewall* com três ou mais portas.

A filtragem de pacotes é composta por uma lista de regras, baseada em correspondências com os campos presentes no cabeçalho IP ou TCP. Ou seja, caso ocorra a correspondência dos campos do cabeçalho com uma das regras, ela é acionada para determinar a transmissão ou o descarte do pacote. Caso não ocorra correspondência com nenhuma das regras, a ação padrão predeterminada é executada. As políticas padrão possíveis são (conforme a Figura 4):

- padrão = descartar, ou seja, tudo o que não for expressamente permitido, será proibido;
- padrão = transmitir, ou seja, tudo o que não for expressamente proibido, será permitido.

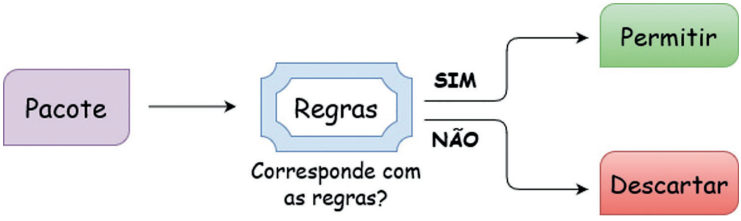

Figura 4. Política padrão filtro de pacote.

Na **política padrão de descartar**, inicialmente tudo é bloqueado, então os serviços devem ser adicionados um por um. Trata-se da política preferida pelas empresas, pois as entradas só serão permitidas a partir da criação das regras. Na **política padrão de transmitir**, a facilidade de uso pelo usuário final aumenta, mas a segurança da rede diminui, pois o administrador de segurança de rede deve tomar ações de acordo com cada ameaça que se torna conhecida.

Exemplo

Stallings e Brown (2014) apresentam um exemplo de regras de filtragem de pacotes em que as regras são aplicadas de cima para baixo e "*" é um coringa, significando "qualquer coisa".

O correio enviado para dentro da rede é permitido (porta 25 é referente ao SMTP de entrada) apenas em uma estação de *gateway*. Porém, os pacotes originados da estação externa EXTEST são bloqueados, devido ao histórico de envios de arquivos maliciosos. Posto isso, o conjunto de regras é determinada da seguinte forma:

Ação	*Host* interno	Porta	*Host* externo	Porta	Comentário
bloquear	*	*	EXTEST	*	fonte não confiável
permitir	INT-GW	25	*	*	conexão com SMTP de entrada

As vantagens do *firewall* de filtro de pacotes incluem sua simplicidade, o fato de geralmente não ser percebido pelos usuários e o fato de ser muito rápido. No entanto, apresenta algumas desvantagens também:

- os filtros de pacotes não examinam dados das camadas superiores, e por isso não conseguem bloquear ataques que explorem vulnerabilidades da camada de aplicação;
- como as informações desse tipo de *firewall* são limitadas, a funcionalidade de registros presentes também são limitadas, limitando as informações de tomadas decisões de controle de acesso;
- a maioria dos *firewalls* de filtro de pacotes não suporta esquemas avançados de autenticação de usuário por não ter acesso às camadas superiores;
- esse tipo de *firewall* é vulnerável a ataques e atividades maliciosas que aproveitam de vulnerabilidades existentes na especificação e na pilha de protocolos TCP/IP, como a falsificação de endereços da camada de rede;
- por fim, como o número de variáveis utilizadas para decisões de controle de acesso é muito pequeno, os *firewalls* de filtro de pacotes são suscetíveis às brechas de segurança que são causadas por configurações incorretas.

Firewall de filtro de pacotes com estado

O *firewall* de filtro de pacotes com estado segue o mesmo princípio do *firewall* de filtro de pacotes, mas podem controlar o tráfego de maneira granular. Diferentemente da filtragem de pacotes, que examina pacotes individuais fora do contexto, a filtragem de pacotes com estado consegue monitorar todo o tráfego de determinada conexão. Uma conexão é definida por endereços IP, portas em uso e tráfego de rede existente.

O *firewall* com estado faz uso de uma tabela de estado, de modo que o estado da conexão seja controlado, e permite apenas o tráfego de uma conexão nova ou já estabelecida. Isso auxilia a evitar tráfegos de ataques que não se assemelham a conexões adequadas que estão sendo esperadas.

É importante destacar que a maioria dos *firewalls* de filtro de pacote com estado também pode funcionar como de filtro de pacote e, em geral, utiliza as duas formas de filtragem conjuntamente. Portanto, além de todos os recursos presentes na filtragem de pacotes, a filtragem de pacotes com estado também pode identificar e rastrear tráfegos relacionados a determinadas conexões já iniciadas pelos usuários com um *site*; dessa forma, será possível identificar quando a conexão for encerrada, de forma que nenhum tráfego legítimo se fará presente. Observe a Figura 5.

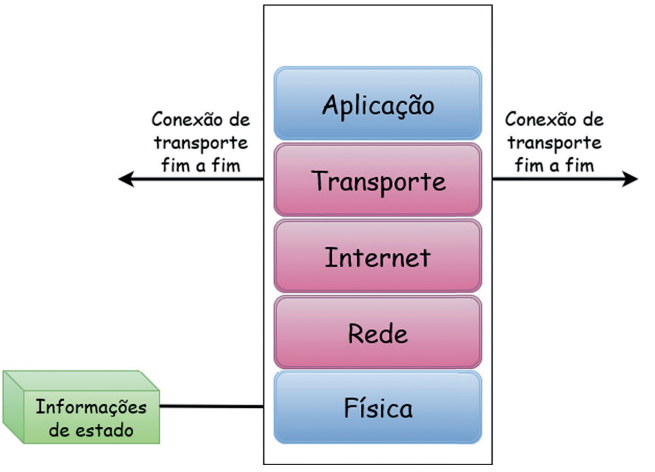

Figura 5. *Firewall* de filtragem de pacotes com estado.
Fonte: Adaptada de Stallings e Brown (2014).

A Figura 5 mostra que o *firewall* de filtragem de pacotes com estado atua filtrando campos que envolvam as camadas de transporte, internet e rede do modelo TCP/IP. Assim, o *firewall* de filtragem de pacotes com estado realiza a análise das mesmas informações de um *firewall* de filtragem de pacotes e registra informações referentes às conexões TCP. Alguns desses *firewalls* também conseguem manter os registros de números de sequência TCP, a fim de impedir ataques que dependam do número de sequência, como o sequestro de sessão, por exemplo.

Esse tipo de *firewall* pode controlar quantidades limitadas de dados de aplicação para determinados protocolos já conhecidos, como comandos FTP (*file transfer protocol*), por exemplo, para a identificação e o rastreamento das conexões relacionadas.

Na próxima seção, descreveremos o funcionamento dos servidores *proxy*.

Servidores *proxy*

O servidor *proxy* é a variação de um *firewall*. Assim como o *firewall*, ele filtra o tráfego, mas age sobre esse tráfego de outras maneiras. Esses servidores são responsáveis por fornecer recursos de segurança e desempenho, nor-

malmente para aplicações, como *e-mail* e navegação *web*. Eles servem como pontos de estrangulamento, permitindo que seja registrado tráfego que passa por eles, para análise posterior, e por isso fornecem camada de segurança para os dispositivos localizados por trás deles. Ou seja, os servidores *proxy* funcionam como uma fonte única de solicitações (ANDRESS, 2014).

Os servidores *proxy* fazem o intermédio entre cliente interno e servidor externo. Além disso, eles ocultam a identidade do solicitante original do servidor por meio do NAT (*network address translation*), que realiza a tradução de endereços IP e portas TCP da rede local para a internet (STEWART, 2014).

Stewart (2014) afirma que o servidor *proxy*, como filtragem de conteúdo, concentra-se em endereços de servidor por meio do nome de domínio ou endereço IP, ou então em palavras-chave que aparecem no contexto da transmissão. Essa forma de filtragem pode ser utilizada para impedir que colaboradores, por exemplo, acessem recursos da internet que não estejam relacionados a suas funções na organização, ou então àqueles que possam ter um impacto direto na rede da empresa, podendo incluir códigos maliciosos, ferramentas de *hacking* e consumo excessivo de largura de banda.

Outra função dos servidores *proxy* é o serviço de cache: um mecanismo de armazenamento de dados que mantém uma cópia local de conteúdo acessado. Geralmente, uma página inicial de um *site* é armazenada em cache por um servidor de *proxy*; então, quando o usuário solicita uma página que se encontra em cache, o servidor *proxy* fornece essa página ao usuário, localizando a cópia local no servidor, em vez de recuperá-la diretamente do *site* sempre que for solicitada. Isso fornece, aos usuários, um maior desempenho e reduz a carga no *link* da internet (STEWART, 2014).

O servidor *proxy* recebe solicitações enviadas a outros servidores e, em seguida, executa serviços, encaminha, redireciona ou rejeita a solicitação. O serviço a ser executado para uma solicitação específica depende de muitos fatores, como da função do servidor *proxy*, do conteúdo da solicitação, das informações contidas na solicitação, de onde veio a solicitação, do destino pretendido e, em determinados casos, de quem enviou o pedido. Ou seja, como esses servidores atuam no intermédio entre estação de trabalho e destino externo, todo tráfego vai para o servidor intermediário, que age como *proxy*. Dessa forma, os dados podem ser analisados e selecionados de maneira adequada antes de serem transmitidos para a infraestrutura de TI. Stewart (2014) apresenta dois tipos de *proxy* que atuam na filtragem de tráfego: proxy de aplicação e *proxy* de circuito, definidos a seguir.

Proxy de aplicação

Também conhecido como *firewall* de aplicação ou *gateway* de aplicação, é uma versão específica de um filtro de pacotes. Ele é capaz de realizar a inspeção do tráfego como um todo em qualquer camada, incluindo carga útil da aplicação, ou seja, realizar uma inspeção profunda de pacotes que envolva todos os aspectos de comunicações de uma aplicação. Por estar entre o cliente e o servidor, todas as comunicações para a aplicação são encaminhadas por meio do *proxy*. Dessa forma, torna-se possível a inspeção de elementos específicos do tráfego da aplicação. Observe a Figura 6.

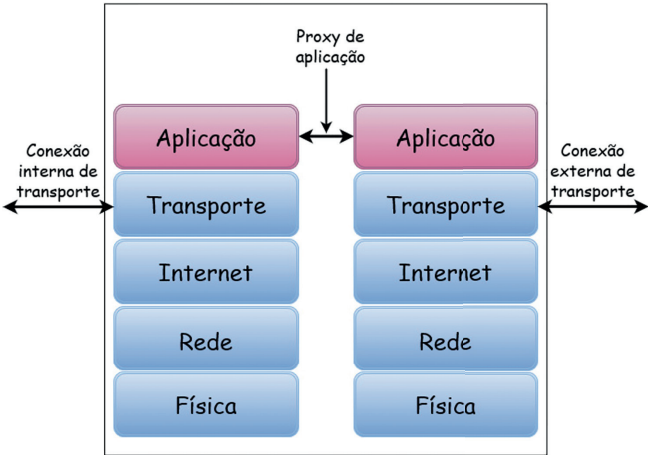

Figura 6. Filtragem com *proxy* de aplicação.
Fonte: Adaptada de Stallings e Brown (2014).

A Figura 6 mostra as camadas do modelo TCP/IP nas quais ocorre a comunicação entre a rede interna e a rede externa, em que o *proxy* de aplicação se encontra entre as camadas de aplicação de ambas as redes, filtrando o tráfego que é permitido e bloqueando o que não é, agindo como um retransmissor de tráfego no nível de aplicação. Assim, o *proxy* de aplicação funciona da seguinte forma: o *proxy* é contatado por um usuário, usando uma aplicação TCP/IP, e solicita, ao usuário, o nome da estação remota a ser acessada. O usuário responde e fornece um ID (*identify*) de usuário válido, além das informações de autenticação. Após isso, o *proxy* contata a aplicação na estação remota, retransmitindo segmentos TCP contendo os dados da aplicação entre as duas extremidades da comunicação. Caso o *proxy* não seja implementado em determinada aplicação, o serviço não será transmitido por meio do *firewall*.

Quando o *proxy* de aplicação é implementado, é necessário que todo o *software*-cliente seja reconfigurado, de modo que as comunicações sejam todas apontadas para o servidor *proxy*, não para o servidor de recursos pretendido. Dessa forma, o *proxy* reconstruirá o pacote de solicitação antes que ele seja encaminhado ao servidor de recursos. É fundamental que os *firewalls* de borda da rede neguem acesso para que os protocolos de aplicação sejam configurados pelo *proxy*, de modo a evitar que usuários consigam ignorá-lo.

A principal limitação desse tipo de *proxy* é que cada aplicação necessita de um próprio *proxy* de aplicação dedicado, gerando um custo adicional de processamento em cada conexão.

Proxy de circuito

O *proxy* de circuito, ou *firewall* de circuito, visa a realizar a filtragem no processo inicial de configuração de uma sessão. A Figura 7 mostra sua localização na rede.

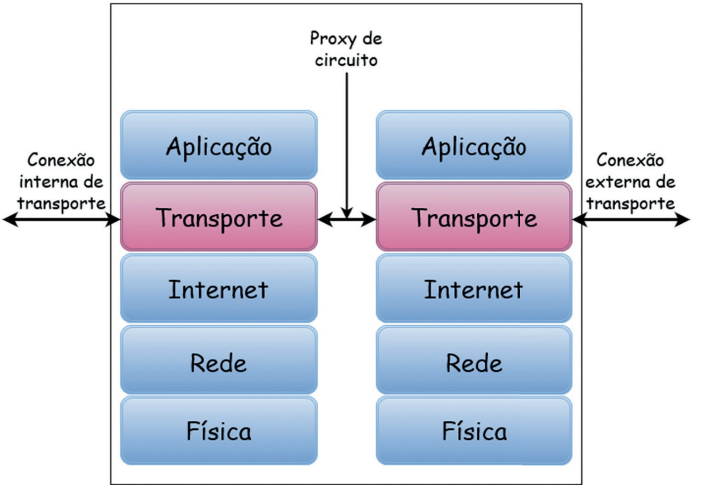

Figura 7. Filtragem com *proxy* de circuito.
Fonte: Adaptada de Stallings e Brown (2014).

A Figura 7 mostra onde o *proxy* de circuito se encontra em uma conexão entre duas redes (interna e externa), sendo representadas pelo modelo de camadas TCP/IP. Ele fica localizado e atua entre as camadas de transporte, funcionando da seguinte forma. O *proxy* de circuito não permite uma conexão TCP fim a fim: ele estabelece duas conexões, uma entre ele mesmo e o usuário

TCP em uma estação interna e outra entre ele e uma estação externa. Após as conexões serem estabelecidas, o *proxy* de circuito transmite os segmentos TCP de uma conexão a outra, mas não realiza a análise do conteúdo enviado. Ou seja, ele apenas toma a decisão de permitir ou negar o início da sessão, estado ou circuito; então, se o usuário tem permissão para iniciar a comunicação, o circuito é criado e nenhuma outra filtragem ocorre por parte dele. Assim, a segurança assegurada pelo *proxy* de circuito consiste em determinar quais conexões serão permitidas.

As regras de filtragem desse tipo de *proxy* devem ser configuradas uma a uma, assim como no *firewall* de filtro de pacotes. Uma lista de regras de endereços IP, números de portas, nomes de domínio, redes ou até provedores de recursos indica como se determinará que circuitos ou conexões serão permitidos e quais não. O conjunto de filtros pode estabelecer posturas de negar tudo, com permitidas exceções, ou posição de permitir tudo, mas negar as exceções.

Com o mercado mais digital a cada dia, torna-se cada vez mais importante investir em soluções de segurança de redes para as organizações. Porém, deve-se ressaltar que, por mais robusta que seja a camada de proteção, sozinha ela não será suficiente. O *firewall* é um dos principais dispositivos utilizados para a segurança de redes; utilizado em conjunto com servidores *proxy*, a proteção é ainda maior. Posto isso, os *firewalls* específicos deverão ser escolhidos de acordo com os recursos da rede, os requisitos de conformidade relevantes e os recursos disponíveis que serão utilizados para gerenciar os *firewalls* implementados.

Referências

ANDRESS, J. *The basics of information security*: understanding the fundamentals of infosec in theory and practice. 2nd ed. Rockland: Syngress, 2014.

HOLMES, D. *et al*. The forrester wave: enterprise firewalls, Q3 2020. 2020. Disponível em: https://reprints2.forrester.com/#/assets/2/154/RES158796/report. Acesso em: 18 jun. 2021.

KIM, D.; SOLOMON, M. G. *Fundamentals of information systems security*. 3rd ed. Jones & Bartlett, 2018.

KIZZA, J. M. *Guide to computer network security*. 5th ed. Berlin: Springer, 2020.

LUTKEVICH, B. *Firewall*. 2021. Disponível em: https://searchsecurity.techtarget.com/definition/firewall. Acesso em: 18 jun. 2021.

PEIXINHO, I. C.; FONSECA, F. M.; LIMA, F. M. *Segurança de redes e sistemas*. Rio de Janeiro: RNP, 2013.

STALLINGS, W.; BROWN, L. *Segurança de computadores*: princípios e práticas. 2. ed. Rio de Janeiro: LTC, 2014.

STEWART, J. M. *Network security, firewalls, and VPNs*. 2nd ed. Burlington: Jones & Barlett, 2014.

STONE, M. *Firewalls explained*: the diferente firewall types and technologies. 2020. Disponível em: https://cybersecurity.att.com/blogs/security-essentials/what-is-a--firewall-types-technologies-explained. Acesso em: 18 jun. 2021.

Fique atento

Os *links* para *sites* da *web* fornecidos neste capítulo foram todos testados, e seu funcionamento foi comprovado no momento da publicação do material. No entanto, a rede é extremamente dinâmica; suas páginas estão constantemente mudando de local e conteúdo. Assim, os editores declaram não ter qualquer responsabilidade sobre qualidade, precisão ou integralidade das informações referidas em tais *links*.

Conteúdo:

SAGAH
SOLUÇÕES EDUCACIONAIS INTEGRADAS