

Firewalls e Detecção de Intrusão

Para começar

Agora estudaremos as ferramentas e tecnologias existentes para enfrentar as ameaças apresentadas nos capítulos anteriores e como garantir os princípios da segurança da informação.

6.1 Introdução

Muitas empresas ao prezarem pela segurança de seus dados decidiram que o uso da internet é restrito àquilo que for necessário para o desempenho do trabalho. É vedado o acesso a redes sociais, sites de entretenimento, jogos ou qualquer outro tipo de passatempo.

Com isso, elas buscam garantir a segurança dos dados corporativos e direcionam o foco dos funcionários para as atividades fins da empresa.

Poderíamos dizer que tal decisão é um exagero em um mundo onde estar conectado é vital para o bem-estar das pessoas. No entanto, como tudo pode ser realizado com equilíbrio, devemos balancear as necessidades da empresa e sua produtividade no ambiente de trabalho com a sua conexão com o mundo exterior.

Analisando do ponto de vista da empresa e da segurança da informação, é claro que encontraremos diversas razões para a existência destes bloqueios no acesso à internet a fim de se estabelecer uma política de segurança e produtividade. Vamos estudar as formas desta utilização e quais os instrumentos de controle para uma maior segurança

6.2 A utilização de acesso à internet em redes corporativas

Atualmente estão disponíveis na internet os mais diversos tipos de conteúdos: notícias em tempo real, sistemas fundamentais para os negócios da empresa, documentos, facilidades financeiras, assim como jogos, salas de bate-papo, redes sociais, vídeos e músicas.

Se analisarmos o acesso ao YouTube®, em razão de seu grande consumo de banda é um fator de preocupação compreensível, já que a rede da empresa deve sempre ter velocidade suficiente para que os funcionários executem suas funções. O acesso intensivo a sites deste tipo, portanto, compromete o desempenho da rede corporativa.

No entanto, a maior preocupação destes acessos está no risco que existe por trás dos links que direcionam para sites ou programas maliciosos, capazes de comprometer o computador e/ou o sistema de uma empresa.

As redes sociais, uma das principais responsáveis por desviarem o foco dos funcionários, também levam a links suspeitos.

Existe um risco potencial para que ocorra a instalação de aplicativos maliciosos, como malware, spyware e vírus, caso o usuário se conecte, sem nenhum controle, a redes sociais.

As empresas se preocupam cada vez mais com a segurança de seus dados e querem que os seus funcionários trabalhem em um ambiente privado e produtivo, e na intenção de evitar problemas, acabam por limitar o acesso a redes como Facebook® e Twitter®, por exemplo.

Se, dentro da empresa, o uso da internet se limita às máquinas corporativas, claro que é possível permitir que os funcionários acessem seus perfis no LinkedIn®, Facebook® e Twitter®, ao mesmo tempo que possam usar o Google para fazer pesquisas em diversos sites ou obter ajuda de um vídeo no YouTube (ou até assistir a um videoclipe para momentos de descontração).

Para que isso ocorra, mesmo que importe em custos adicionais, bastará a empresa proteger os seus computadores e as suas redes contra ataques maliciosos e orientar os funcionários quanto ao uso da internet: *afinal, quando se está trabalhando, é preciso ter bom senso e evitar dispersão.*

Para contornar estas questões de acesso indiscriminado à internet nos computadores corporativos, muitas, se não a maior parte das empresas, utilizam ferramentas como firewalls.

6.3 O que é um firewall?

Firewall é um mecanismo de segurança realizado em *hardware* ou *software* (que é o mais utilizado) que possui/implementa um conjunto de regras ou instruções, faz a análise do tráfego de rede (tudo o que passa na rede em que estamos conectados) e determina de acordo com as regras implementadas quais são as operações de transmissão ou recepção de dados que podem ser executadas.

“Parede de fogo”, a tradução literal do nome, já deixa claro que o firewall se enquadra em uma espécie de barreira de defesa.

O objetivo de um firewall é bloquear qualquer tráfego de dados indesejado e não autorizado e liberar somente os acessos autorizados.

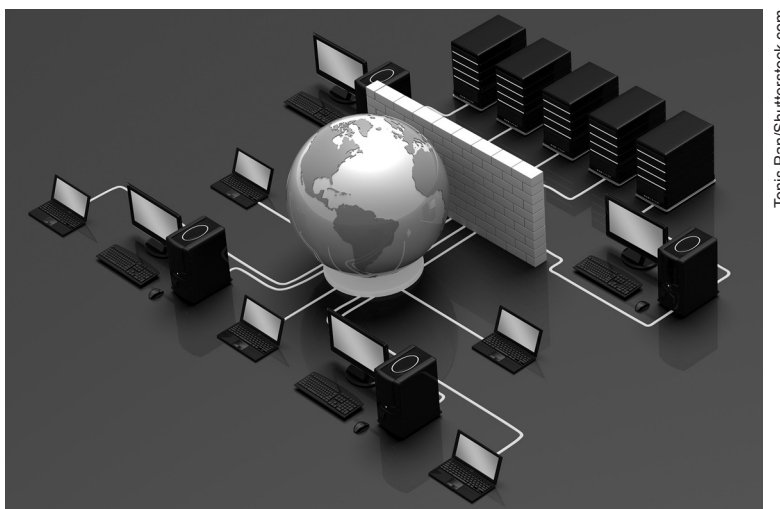


Figura 6.1 – Representação básica de um firewall.

Um dos melhores exemplos que encontrei sobre o que seria equivalente a um firewall na vida real está a seguir. Sem dúvida permitirá entender claramente a finalidade de um firewall:

“... você pode imaginar um firewall como sendo uma portaria de um condomínio: para entrar, é necessário obedecer a determinadas condições, como se identificar, ser esperado por um morador e não portar qualquer objeto que possa trazer riscos à segurança; para sair, não se pode levar nada que pertença aos condôminos sem a devida autorização.”

ALECRIM, Emerson. *O que é firewall? – Conceito, tipos e arquiteturas*. Publicado em 19_02_2013. Disponível em: [em <http://www.infowester.com/firewall.php>](http://www.infowester.com/firewall.php). Acesso em: 10 mar. 2014.

Devemos entender que um firewall é utilizado para restringir os acessos em uma rede por outra rede, ou seja, por usuários de outra rede. O firewall não tem atuação interna nos acessos dentro da própria rede. Estes controles são relativos aos controles de acesso, identificação e validação de usuários da própria rede.

Entretanto, podemos aplicar um firewall para restringir acesso a um segmento de uma rede interna pelos usuários desta rede corporativa.

Um firewall é uma ferramenta que suporta e reforça uma política de segurança de rede, que fornecerá instruções de alto nível sobre as ações aceitáveis e não aceitáveis no que se refere à segurança.

Um firewall é utilizado para impedir a execução de ações maliciosas oriundas de outra rede: um malware que utiliza determinada entrada lógica (porta) para se instalar em um computador sem o usuário saber e nem perceber, ou um programa que envia dados sigilosos da empresa para a internet. Ou, finalmente, o mais comum, uma tentativa de acesso à rede de uma empresa, ou sua rede doméstica, a partir de computadores externos não autorizados.

6.3.1 Como um firewall funciona?

Já estudamos que um firewall atua como uma barreira que verifica quais dados podem passar ou não, e que esta tarefa só pode ser realizada pelo estabelecimento de regras, chamadas políticas de segurança.

As ações de um firewall têm basicamente duas regras:

- » Todo tráfego é bloqueado, exceto o que está explicitamente autorizado;
- » Todo tráfego é permitido, exceto o que está explicitamente bloqueado.

Firewalls podem ir além, direcionando determinado tipo de tráfego para sistemas de segurança internos mais específicos ou atuando como um reforço nos procedimentos de autenticação de usuários.

Para entendermos melhor, considere que a complexidade de instalação de um firewall depende do tamanho da rede que ele irá proteger, da política de segurança que a empresa irá implementar, da quantidade de regras que forem implementadas para controlar o fluxo de entrada e saída de informações que passarem por ele. Além disso, é importante termos em mente que ele deverá garantir o grau de segurança desejado em uma rede.

6.3.2 Tipos de firewall – Firewall em forma de softwares

O trabalho de um firewall pode ser realizado de várias formas. O que define uma metodologia ou outra são fatores como critérios do desenvolvedor, necessidades específicas do que será protegido, características do sistema operacional que o mantém, estrutura da rede e assim por diante. É por isso que podemos encontrar mais de um tipo de firewall.

Elencaremos, a seguir, os mais conhecidos.

6.3.2.1 Filtragem de pacotes (packet filtering)

As primeiras soluções de firewall surgiram na década de 1980, baseando-se em **filtragem de pacotes** de dados, uma metodologia mais simples e relativamente limitada, embora ofereça um nível de segurança significativo.

Pacotes de dados são a estrutura unitária de transmissão de dados ou uma sequência de dados transmitida por uma rede.

Para entendermos melhor: cada pacote de dados possui um cabeçalho com diversas informações a seu respeito, como endereço IP de origem, endereço IP do destino, tipo de serviço, tamanho, entre outros.

O firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log, o que criará um histórico de todas as operações que trafegaram em uma rede por meio do firewall.

A transmissão dos dados é feita com base no padrão TCP/IP (*Transmission Control Protocol/Internet Protocol*), que é organizado em camadas.



Figura 6.2 – Filtragem de pacotes.

A filtragem normalmente se limita às camadas de rede e de transporte: a primeira é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e os processos de roteamento, por exemplo. A segunda, onde estão os protocolos que permitem o tráfego de dados, como o TCP.

Importante voltarmos a salientar que a comunicação pela internet é feita, basicamente, por meio de protocolos de comunicação, sendo o TCP (*Transmission Control Protocol*) um dos mais importantes deles, se não o mais importante. Isso porque o TCP está incluído no conjunto de protocolos que formam o TCP/IP, a base de comunicação via dados de toda a internet.

Para reforçarmos o conteúdo apresentado, apresentamos as principais características do TCP:

- » **Garante a entrega de pacotes de dados IP:** esta talvez seja a principal função do TCP, ou seja, garantir que os pacotes sejam entregues sem alterações, sem terem sido corrompidos e na ordem correta. O TCP tem uma série de mecanismos para garantir esta entrega.
- » **Executa a segmentação e o reagrupamento de grandes blocos de dados enviados pelos programas e garante o sequenciamento adequado e a entrega ordenada de dados segmentados:** esta característica refere-se à função de dividir grandes arquivos em pacotes menores e transmitir cada pacote separadamente. Os pacotes podem ser enviados por caminhos diferentes e chegar fora de ordem. O TCP tem mecanismos para garantir que, no destino, os pacotes sejam ordenados corretamente antes de serem entregues ao programa de destino.
- » **Verifica a integridade dos dados transmitidos usando cálculos de soma de verificação:** o TCP faz verificações para garantir que os dados não foram alterados ou corrompidos durante o transporte entre a origem e o destino, verificando o hash dos pacotes.
- » **Envia mensagens positivas, dependendo do recebimento bem-sucedido dos dados.** Ao usar confirmações seletivas, também são enviadas confirmações negativas para os dados que não foram recebidos: no destino, o TCP recebe os pacotes, verifica se estão OK e, em caso afirmativo, envia uma mensagem para a origem, confirmando cada pacote que foi

recebido corretamente. Caso um pacote não tenha sido recebido ou tenha sido recebido com problemas, o TCP envia uma mensagem ao computador de origem, solicitando uma retransmissão do pacote. Com esse mecanismo, apenas pacotes com problemas terão de ser reenviados, o que reduz o tráfego na rede e agiliza o envio dos pacotes.

- » Oferece um método preferencial de transporte de programas que devem usar transmissão confiável de dados baseada em seções, como bancos de dados cliente/servidor e programas de correio eletrônico: ou seja, o TCP é muito mais confiável do que outros protocolos e é indicado para programas e serviços que dependam de uma entrega confiável de dados.

Fonte: definição dada por Júlio Battisti em artigo publicado na JB Livros e Cursos, disponível em http://www.juliobattisti.com.br/artigos/windows/tcpip_p11.asp.

Com base nisso, um firewall de filtragem pode ter, por exemplo, uma regra que permita todo o tráfego da rede local que utilize a porta TCP 80, assim como ter uma política que bloqueia qualquer acesso da rede local por meio da porta TCP 25.

Você deve estar agora se perguntando, mas o que é uma porta no computador?

Para entendermos o conceito de porta, imaginemos um computador, de uma empresa ou pessoal, com conexão à internet.

Você pode, ao mesmo tempo, acessar um ou mais sites, usar o Microsoft Outlook® para ler ou enviar mensagens de e-mail. Ou se estiver em casa, jogar online, digamos, Resident Evil 4®.

Todas as informações recebidas vêm por meio de pacotes de dados que chegam até a placa de rede ou até o Modem DSL, no caso de uma conexão de banda larga doméstica. A pergunta que naturalmente surge é: como o sistema operacional do computador entende para qual dos programas se destina cada um dos pacotes de dados que estão chegando ou saindo? Na chegada de determinado pacote, como o sistema operacional do computador sabe se este pacote é para uma janela específica aberta no meu browser, uma mensagem de e-mail, quem é o destinatário deste e-mail, ou então se não é um comando executado no Resident Evil 4®?

Cada programa trabalha com um protocolo/serviço específico, ao qual está associado um número de porta.

Logo o protocolo TCP/IP possui um conjunto de portas a que ele está associado.

Outro exemplo, o protocolo HTTP, utilizado para transportar as informações de um site que está em um servidor Web até o seu browser, trabalha, por padrão, na porta 80.

Assim todos os pacotes de dados que chegarem destinados à porta 80 serão encaminhados para o browser de internet.

É a existência do conceito de portas que nos permite utilizar vários serviços ao mesmo tempo na internet.

Embora isso também possa representar alguns perigos, é importante ter controle sob o tráfego de dados nas portas TCP. Este controle pode ser obtido por meio da utilização de firewalls, como

impedir que programas maliciosos utilizem as portas abertas no computador para atividades mal-intencionadas.

Amplie seus conhecimentos

Caso você queira se aprofundar neste assunto, recomendamos pesquisar e estudar sobre TCP/IP e camadas OSI.

Algumas fontes de pesquisa são:

www.joinville.udesc.br/sbs/professores/erivelto/.../Modelo_TCPIP.ppt

www-usr.inf.ufsm.br/~candia/aulas/espec/Aula_3_Modelo_OSI.pdf

www.telecomhall.com/BR/modelo-de-7-camadas-osi.aspx

6.3.2.2 Filtragens estática e dinâmica

É possível encontrar dois tipos de firewall de filtragem de pacotes.

O primeiro utiliza o que é conhecido como *filtros estáticos*, enquanto o segundo é um pouco mais evoluído, utilizando *filtros dinâmicos*.

Mas o que são estas filtragens?

Na filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras implantadas no firewall, não importando a ligação que cada pacote tem com o outro.

A princípio, esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão.

É possível então que os filtros conttenham regras que permitem o tráfego destes serviços, mas, ao mesmo tempo, bloqueiem as respostas/requisições necessárias, impedindo a execução completa de uma tarefa.

Esta situação é capaz de ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, e com isso aumentar os riscos de o firewall não filtrar pacotes que deveriam ser, de fato, bloqueados.

A filtragem dinâmica surgiu para superar as limitações existentes nos filtros estáticos.

Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para “criar” regras que se adaptem aos cenários, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante um período correspondente.

Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

6.3.2.3 Firewall de aplicação ou proxy de serviços (Proxy)

Você já deve ter ouvido falar em servidor Proxy, um tipo de firewall.

O objetivo principal de um servidor Proxy é permitir que os computadores de uma rede possam acessar uma rede pública, como é denominada a internet, sem que seja necessário ter uma ligação direta com esta, mantendo-se assim o controle do que é acessado.

O **firewall de aplicação**, também conhecido como **Proxy** de serviços (*proxy services*) ou apenas **Proxy**, é uma solução de segurança que atua como um intermediário entre um computador ou uma rede interna e outra rede, na maioria dos casos uma rede externa – normalmente, a internet.

Geralmente o Proxy é instalado em servidores potentes que se conectam a internet, porque cabe a eles não permitir que seja realizada a comunicação direta entre uma origem e um destino.

Grave bem este diferencial!

O Proxy atua como sendo o procurador das outras máquinas, pois ele é quem faz as solicitações de acesso à web no lugar delas.

A Figura 6.3 ajuda na compreensão do conceito.

Perceba que, em vez de a rede interna se comunicar diretamente com a internet, há um equipamento entre ambos que cria duas conexões: entre a rede e o Proxy, e entre o Proxy e a internet.

Observe:

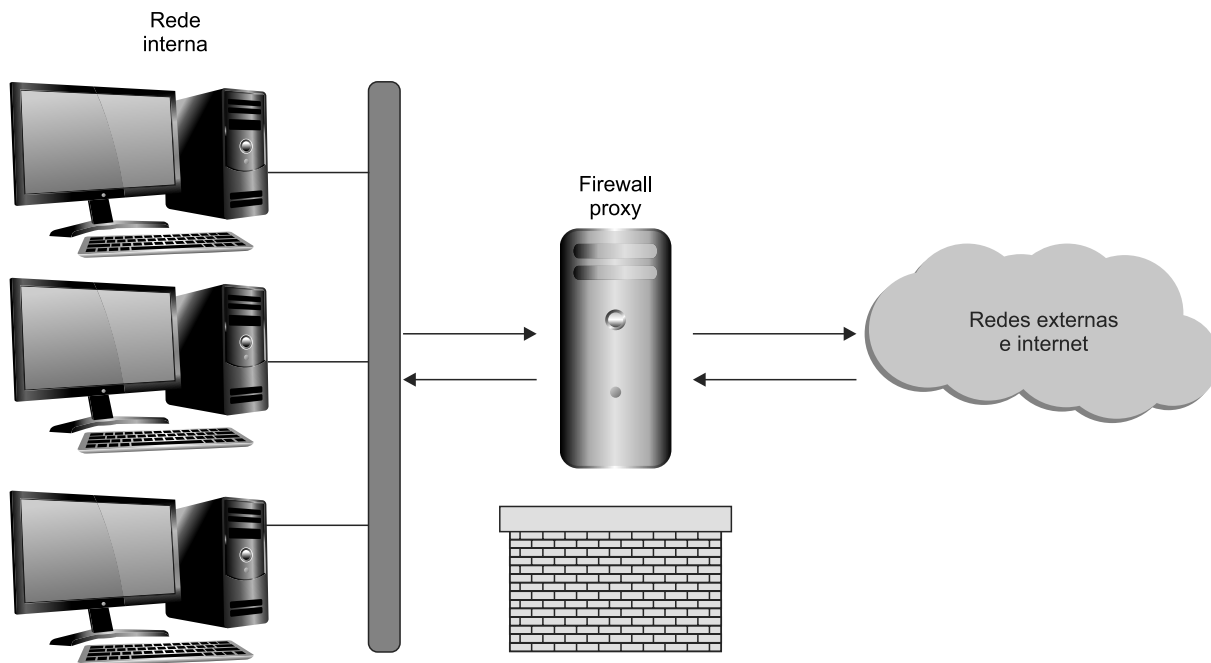


Figura 6.3 – Firewall Proxy.

Perceba que todo o fluxo de dados necessita obrigatoriamente passar pelo **Proxy**.

Desta forma, é possível, por exemplo, estabelecer regras que impeçam o acesso de determinados endereços externos e que proíbam a comunicação entre computadores internos e determinados serviços remotos.

Este controle amplo também possibilita o uso do **Proxy** para tarefas complementares: o equipamento pode registrar o tráfego de dados entre as redes, em um arquivo de log. Desta forma conteúdos muito utilizados podem ser guardados em uma espécie de cache⁶ (uma página da Web muito acessada fica guardada temporariamente no Proxy, fazendo com que não seja necessário requisitá-la e acessá-la no endereço original a todo instante, por exemplo). Alguns recursos podem ser liberados apenas mediante autenticação do usuário.

A implementação de um **Proxy** não é uma tarefa fácil, haja vista a enorme quantidade de serviços e protocolos existentes na internet, fazendo com que, dependendo das circunstâncias, este tipo de firewall exija muito trabalho de configuração para bloquear ou autorizar uma gama muito grande de determinados tipos de acessos.

Normalmente um **Proxy** direciona as solicitações da rede para uma porta específica. Porém, para isso, utilizamos o que é denominado de Proxy transparente, ou seja, para os usuários é transparente esta passagem pelo mesmo, mas a mesma fica obrigatória por esta configuração.

Nenhuma solicitação de acesso externo é executada e atendida sem passar pelo Proxy.

Amplie seus conhecimentos

Pesquise sobre ferramentas de bloqueio de acesso a sites baseadas na nomenclatura do domínio, tipo SQUID, por exemplo. Você irá com certeza ampliar seu horizonte de ferramentas para implementação de segurança com Proxy.

Pesquise sobre como é colocado em uma rede um Proxy transparente. Olhe as configurações de internet no Painel de Controle de seu computador em casa ou na empresa.

6.3.2.4 Inspeção de estados (stateful inspection)

Tido por alguns especialistas no assunto como uma evolução dos filtros dinâmicos, os firewalls de **inspeção de estado** (*stateful inspection*) fazem uma espécie de comparação entre o que está acontecendo e o que é esperado para acontecer.

Para tanto, os firewalls de inspeção analisam todo o tráfego de dados para encontrar estados, isto é, padrões aceitáveis por suas regras e que, a princípio, serão usados para manter a comunicação estável e segura.

Estas informações são mantidas pelo firewall e usadas como parâmetro para todo o tráfego de dados subsequente.

Para entendermos melhor, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um computador cliente e um computador servidor.

Os pacotes de dados iniciais informam quais portas TCP serão usadas para esta tarefa.

⁶ Cache é uma área temporária para armazenamento de dados de um programa, ou do próprio sistema operacional do computador. O cache de memória funciona como uma extensão da memória, também sendo utilizado para guardar dados temporários e permitir acesso rápido a eles.

Se de repente o tráfego começar a fluir por uma porta não mencionada, o firewall pode então detectar esta ocorrência como uma anormalidade, pois o estado da comunicação mudou para um estado não esperado, e assim ele bloqueará este tráfego de dados.

6.3.2.5 Firewalls pessoais

Mas há firewalls mais simples, destinados a proteger o seu computador, seja ele um desktop, um laptop ou um tablet.

São os **firewalls** pessoais (ou domésticos), que DEVEM ser utilizados por qualquer pessoa.

Felizmente, os sistemas operacionais de uso doméstico ou em escritório normalmente contêm um firewall interno padrão, como é o caso do Linux, do Windows (Firewall do Windows), em todas as suas últimas versões, ou do Mac OS X.

Além disso, é comum desenvolvedores de antivírus oferecerem outras opções de proteção junto ao software, entre elas, um firewall.

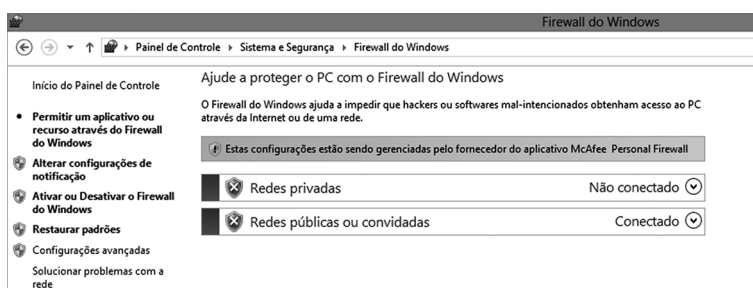


Figura 6.4 – Firewall do Windows.

6.3.2.6 Firewalls de conteúdo

Quando um site é acessado por meio de um firewall de conteúdo (por exemplo, *dansguardian*), ele analisa o seu conteúdo em função de uma lista de regras predefinidas e configuráveis pelo administrador do firewall que permitem ou bloqueiam os acessos.

Assim é possível bloquear o acesso a sites indesejáveis, impedir o download de determinados tipos de arquivos ou evitar a propagação de vírus.

Neste item podemos escolher qual é o tipo de conteúdo a ser bloqueado, pois o software utilizado funciona por meio de análise de conteúdo. Seleccionamos, então, as opções que desejamos bloquear dentre as várias que nos são apresentadas, como pornografia, chats, games etc., por intermédio da inserção de regras que têm como base palavras-chave na composição da nomenclatura do site: %sports%; %sex%, entre outras.

6.3.2.7 Firewall de hardware

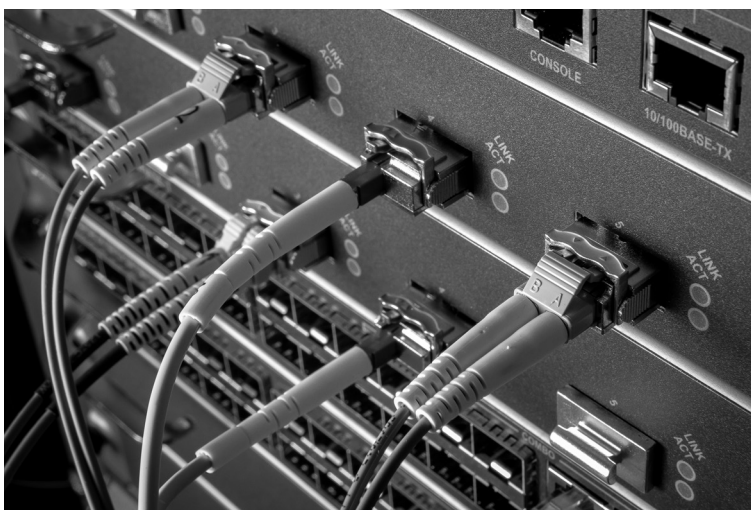
No início deste tema destacamos que um firewall pode ser uma solução de software ou hardware.

Esta informação não está incorreta, mas é necessário um complemento: o hardware nada mais é do que um equipamento com um software de firewall instalado.

É possível encontrar, por exemplo, roteadores ou equipamentos semelhantes a um firewall que exercem a função em questão.

Neste caso, o objetivo é proteger uma rede, normalmente de grandes empresas, com tráfego muito acentuado, ou em grandes volumes, ou com dados muito importantes.

A vantagem de um firewall de hardware é que o equipamento, por ser desenvolvido especificamente para este fim, é preparado para trabalhar com grandes volumes de dados e não está sujeito às vulnerabilidades que eventualmente podem ser encontradas em um servidor convencional (por conta de uma falha em outro software, por exemplo).



kubai/Shutterstock.com

Figura 6.5 – Firewall de hardware.

Outra vantagem quando se utilizam equipamentos desse tipo é que o hardware é dedicado à segurança, às funções de firewall, em vez de compartilhar recursos com outros aplicativos.

Dessa forma, o firewall de hardware pode ser capaz de tratar mais requisições e aplicar os filtros de maneira mais ágil.

Estes equipamentos são chamados de UTM (Unified Threat Management – Gerenciamento unificado de ameaças) e contam com recursos de filtro de pacotes, proxies, antivírus, antispam, concentrador VPN, filtro de conteúdo, IDS/IPS; e em soluções mais robustas, com a capacidade de roteamento avançado, balanceamento de carga de tráfego de rede e extensas possibilidades de relatórios e monitoramento.

A maioria dos roteadores de rede de banda larga domiciliar Wi-Fi disponíveis também contam com algum tipo de aplicação de firewall.

Uma das mais básicas é o controle sobre os computadores que estão habilitados a se conectar na rede. Elas impedem que “sanguessugas” de plantão usem a sua rede Wi-Fi sem permissão, pois necessitam da chave de acesso deste roteador para conectar na sua rede Wi-Fi e acessar a internet.

Você pode aprender mais sobre a segurança de redes sem fio e firewalls, em sites como:

- » www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm;
- » www.abchost.cz/download/204-4/.../-inspection-firewall.pdf.

6.3.3 Limitações dos firewalls

Você já deve ter notado, mesmo com todos os aspectos destacados, que os firewalls também têm suas limitações, que variam conforme o tipo de solução e a arquitetura e topologia de rede utilizadas.

De fato, firewalls são recursos de segurança extremamente importantes, principalmente em redes de empresas. No entanto, eles não são perfeitos, isto é, não existe nenhuma rede 100% segura, mesmo protegida por um firewall.

Resumidamente, podemos mencionar as seguintes limitações:

- » Um firewall sempre oferece a segurança desejada, desde que esta segurança esteja bem definida e não venha a comprometer o desempenho da rede (ou mesmo de um computador). Situações como esta geram às vezes um custo mais elevado, nos casos em que desejarmos realizar uma ampliação dos recursos tecnológicos de infraestrutura com a finalidade de atender a uma necessidade específica da área tecnológica;
- » A verificação de políticas de segurança e restrições de acesso tem que ser revista periódica e constantemente para não prejudicar o funcionamento de novos serviços e sistemas necessários para uma empresa;
- » Nem sempre novos serviços ou protocolos implementados em uma rede podem estar sendo tratados corretamente pelos proxies já implementados até aquele momento;
- » Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede interna (muita atenção a este detalhe, **atividade maliciosa de origem interna à rede**);
- » Um firewall pode não ser capaz de identificar uma atividade maliciosa que acontece por descuido do usuário – quando o usuário, ao clicar em um link de uma mensagem de e-mail, acessa um site falso de um banco, por exemplo (destacamos aqui a questão da interação das pessoas nos problemas de segurança da informação);
- » Firewalls precisam ser “vigiados”, acompanhados permanentemente por pessoas responsáveis e sempre atualizados, porque atacantes experientes podem tentar descobrir ou explorar brechas de segurança;
- » Um firewall não pode interceptar uma conexão que não passa por ele. Se, por exemplo, um usuário acessar a internet em seu computador a partir de uma **conexão 3G** (para, quem sabe, burlar as restrições da rede), o firewall com certeza não conseguirá interferir e garantir a segurança normal, pois não existirá a passagem deste acesso através do firewall

da rede, já que estará sendo realizado um acesso à internet por uma conexão externa à rede, ocorrendo o mesmo fora dos controles existentes no ambiente de rede.

Como você pôde aprender até aqui neste capítulo, os firewalls são soluções importantes de segurança – não é à toa que surgiram na década de 1980 e são amplamente utilizados até os dias de hoje.

Mas, tal como evidenciam as limitações apresentadas, um firewall não é capaz de proteger totalmente uma rede ou um computador, razão pela qual deve ser utilizado sempre em conjunto com outros recursos, como antivírus, sistemas de detecção de intrusos, entre outros.

Utilizar um firewall serve tanto para aplicações empresariais quanto para domiciliar, protegendo não só a integridade dos dados na rede, mas também a confidencialidade destes dados.

O pensamento que devemos ter é: *utilizar um firewall é parte da implementação de segurança da informação, mas não é a segurança em si.*

De nada adianta um portão com câmera, na entrada do seu prédio, se além disso não tivermos o pessoal de monitoramento acompanhando. Ou seja, nada funciona sozinho, somente com atuações em conjunto podemos conseguir resultados mais satisfatórios.

Você deve seguidamente se perguntar por que pegamos vírus, por que a internet em alguns casos não tem seu rendimento como esperado em nossa empresa.

A resposta é relativamente simples, segundo Emerson Alecrim:

Nos casos em que temos 100% dos conteúdos liberados perdemos inevitavelmente produtividade por meio de alguns acessos comuns, como Facebook®, YouTube®, Twitter®, entre outros.

Fonte: Emerson Alecrim. Publicado em: 19 fev. 2013. Atualizado em: 19 fev 2013 em <http://www.infowester.com/firewall.php>.

6.3.3.1 Políticas de segurança para firewalls

Um firewall fornece os meios para implementação e aplicação de uma política de segurança no acesso à rede. Este talvez seja o mais importante dos aspectos a considerarmos.

De fato, um firewall fornece controle de acesso de usuários e serviços.

Assim, uma política de acesso à rede pode ser aplicada por um firewall, visto que, sem um firewall, uma política de acesso à rede depende exclusivamente da cooperação e boa vontade dos usuários.

Um site pode ser capaz de depender de seus próprios usuários e da sua cooperação. Entretanto, não pode nem deve depender de usuários da internet em geral.

Existem dois níveis de política de rede que influenciam diretamente na concepção, instalação e utilização de um firewall em uma rede.

A primeira é o que denominamos de política de nível superior. Em outras palavras, trata-se de uma política que define o acesso à rede, contendo as questões específicas que definem quais serviços serão permitidos, quais serviços serão explicitamente negados em uma rede restrita, como esses serviços serão utilizados e quais as condições de exceção a essa política de utilização. Toda regra sempre tem uma exceção.

A seguir temos uma segunda política, de nível mais baixo, que descreve como o firewall irá realmente restringir os acessos e as filtragens dos serviços que forem definidos na política de nível superior.

A política de acesso aos serviços deve se concentrar em questões de uso específico da internet e, principalmente, em todos os acessos a redes do lado de fora.

Esta política deve ser uma extensão de uma política global da organização em matéria de proteção dos recursos de informação na organização.

Para que um firewall seja bem-sucedido, a política de acesso aos serviços deve ser e tem de ser elaborada antes da implementação de um firewall.

Uma política realista é aquela que fornece um equilíbrio entre proteger a rede de riscos conhecidos, enquanto continua a fornecer aos usuários disponibilidade de acesso a recursos de rede.

Se um firewall nega ou restringe serviços, normalmente ele requer que exista a força de uma política de segurança de acesso aos serviços para evitar que os controles de acesso do firewall sejam modificados de forma ad hoc, somente em função de interesses momentâneos ou pessoais.

Outra medida bastante utilizada diz respeito aos filtros por portas e aplicativos. Com eles, o firewall pode determinar, exatamente, quais programas do seu computador podem ter acesso ao link de internet ou não.

As portas de comunicação também podem ser controladas por você, leitor, da mesma forma, permitindo que as portas mais “visadas” pelos malwares sejam bloqueadas terminantemente.

Outra política típica seria permitir algum acesso a partir da internet, mas apenas para sistemas selecionados, como servidores de busca de informação e servidores de e-mail.

Firewalls costumam implementar políticas de acesso de serviços que permitem algum tipo de acesso do usuário a partir da internet para hosts internos selecionados. Esse acesso, contudo, será concedido apenas se necessário e somente se ele puder ser combinado com uma forma de autenticação avançada.

O que desejamos até este ponto do livro é que você, leitor, se acostume com os termos e o objeto política de acessos. É por meio da garantia máxima de segurança de acessos a uma rede, seja interna ou externamente, que buscamos manter a segurança da informação.

Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, como o Windows 8, garantindo a segurança do computador desde o momento em que ele é ligado pela primeira vez, e inclusive com intersecção com um programa antivírus tipo McAfee Internet Security®.

Os firewalls trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados e entregues ao destino e com que todos os outros fora das regras nunca cheguem ao destino final.

Amplie seus conhecimentos

Você pode aprender mais sobre a segurança de redes sem fio em artigos na internet, pesquise <http://www.tecmundo.com.br/firewall/182-o-que-e-firewall-.htm#ixzz2sXY0SPFH>.

6.4 Sistemas de detecção de intrusão

Sistemas de Detecção de Intrusão (IDS) são usados para monitorar uma rede ou computadores individuais.

O IDS tem por finalidade detectar uma ameaça ou intrusão na rede.

Pode-se dizer por analogia que um IDS é como se fosse um alarme de uma casa ou de seu carro que toca quando alguém abre a porta.

6.4.1 Mas o que são intrusos?

Intrusos são os invasores (hackers) de um sistema e podem ser classificados em três tipos:

- » **Mascarado** (invasor de fora da rede ou sistema): alguém que não está autorizado a entrar no sistema e o invade para obter privilégios de um usuário legítimo;
- » **Infrator** (invasor de dentro da rede): é um usuário real ou legítimo que não está autorizado a usar determinados recursos, mas os utiliza, ou que está autorizado, mas não os utiliza de forma lícita, sendo considerado mal-intencionado;
- » **Usuário clandestino** (invasor de dentro ou de fora da rede): invasor que toma posse de privilégios de administrador de sistema para escapar das auditorias e dos controles de acesso ou até mesmo para alterar registros de auditorias contra ele.

6.4.2 Tipos de sistemas de detecção de intrusão

Existem dois tipos principais de Sistemas de Detecção de Intrusão: (1) baseados em rede e que monitoram uma rede ou um segmento de uma rede; e (2) baseados em host, isto é, que monitoram um sistema em particular.

O Sistemas de Detecção de Intrusão em host é instalado em uma determinada máquina (servidor) para avaliar o próprio host. Ele analisa os eventos do sistema operacional, eventos de acesso e eventos de aplicações, monitora as entradas, ou qualquer outra parte que represente tentativa de intrusão. Além disso, bloqueia ataques que não são detectados pelo firewall, como protocolos criptografados. Um IDS deste tipo também acusa uma tentativa suspeita, como um usuário tentando utilizar algo para o qual ele não tenha permissão.

Ele pode ser configurado para observar ataques de crackers, analisar logs de auditoria, alertar um administrador sobre os ataques sendo realizados, proteger os arquivos do sistema, expor as técnicas utilizadas por um cracker e as vulnerabilidades que precisam ser abordadas, corrigidas e, possivelmente, ajudar a rastrear alguns hackers individuais.

Os Sistemas de Detecção de Intrusão baseados em rede (NIDS) são geralmente usados para garantir que usuários não excluam “acidentalmente” arquivos do sistema, redefinam alguma configuração importante ou venham a colocar em risco os sistemas de alguma outra maneira.

Um NIDS é instalado normalmente em um segmento de rede, onde uma base de dados faz as comparações necessárias com os pacotes de rede ou então faz a decodificação e verifica os protocolos de rede.

Os IDS baseados em rede verificam os usuários externos não autorizados a entrar na rede, tentativas de ataques de negação de serviços (DoS) ou roubo de alguma base dados.

Este mesmo tipo de IDS monitora o tráfego de pacotes de rede para descobrir possíveis ataques ou atividades suspeitas, e isso normalmente é feito pela detecção de anomalias e pela identificação de padrões.

O conhecimento é acumulado sobre ataques específicos e como eles são realizados. Modelos desses ataques são desenvolvidos e chamados de assinaturas de ataques. Cada ataque tem uma assinatura, que é utilizada depois para detectar a ocorrência de um novo ataque, caso já tenha ocorrido alguma vez no interior da rede.

Se o volume de tráfego de rede exceder o limite que o sistema IDS suporta, os ataques podem passar despercebidos. Todos os produtos de sistema IDS de qualquer fornecedor têm o seu próprio limite, que devem ser conhecidos e bem compreendidos antes de comprar e configurar o produto de software.

São exemplos de Sistemas de Detecção de Intrusão baseados em rede: RealSecure, NFR e Snort.

São exemplos de Sistemas de Detecção de Intrusão baseados em host: Tripware, Swatch e Portsentry.

Amplie seus conhecimentos

Pesquise e liste as vantagens e desvantagens dos tipos de Sistemas de Detecção de Intrusão Tripware e NFR:

<https://tripwire.dhs.gov/>

www.trtec.com.br/pages/nfr.html

6.4.3 Implementação de sistemas de detecção de intrusão na rede

É comum colocar-se um IDS antes do firewall para impedir que um usuário externo conheça qual é a topologia da rede, e um depois do firewall, em uma área denominada desmilitarizada, para identificar algum ato que o firewall não tenha detectado.

Em instalações de empresas também é normal colocar-se um IDS para detectar ataques advindos da rede interna e, por fim, colocar um HIDS (baseado em host) para aqueles servidores considerados de maior risco a ataques, como o WebServer e os servidores de email.

A Figura 6.6 apresenta uma rede com Sistemas de Detecção de Intrusão antes do firewall e após o firewall, com Sistemas de Detecção de Intrusão de host para os servidores de e-mail e servidor Web.

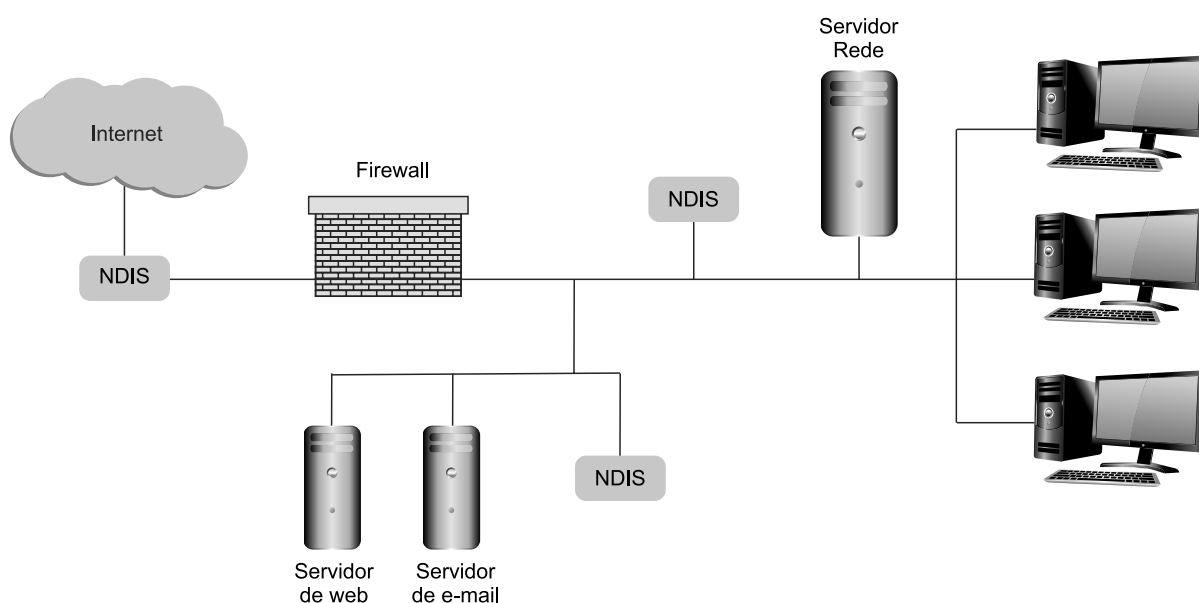


Figura 6.6 – Arquitetura de Sistemas de Detecção com utilização de NDIS e HIDS.

Vamos recapitular?

Neste capítulo aprendemos o que são os firewalls, para que eles servem, quais são suas formas e tipos, assim como sobre a importância da elaboração e existência de uma política de acessos a redes e à internet a partir de uma rede interna, seja ela de uma empresa ou doméstica de banda larga.

Estudamos também o funcionamento dos sistemas de detecção de intrusão em redes. Nos próximos capítulos vamos estudar outras formas bastante importantes no controle de acessos, como as regras de identificação de usuários e criação de senhas de acesso a redes, bancos de dados etc.



Agora é com você!

- 1) A utilização de firewalls abarca quais princípios da segurança da informação?
- 2) Qual tipo de controle controla e bloqueia a entrada de usuários estranhos à rede da empresa?
- 3) Pesquise em sua escola e relacione como estão implementados os firewalls na rede, e faça uma síntese destes processos.
- 4) O acesso a sites como Facebook pode ser bloqueado por um firewall, ou necessariamente temos de ter um software de proxy para este fim?
- 5) Um firewall monitora o tráfego que entra e sai e filtra, redireciona, reempacota e/ou rejeita pacotes de dados?
- 6) Quando queremos monitorar também pacotes criptografados, podemos utilizar um firewall para proteção?