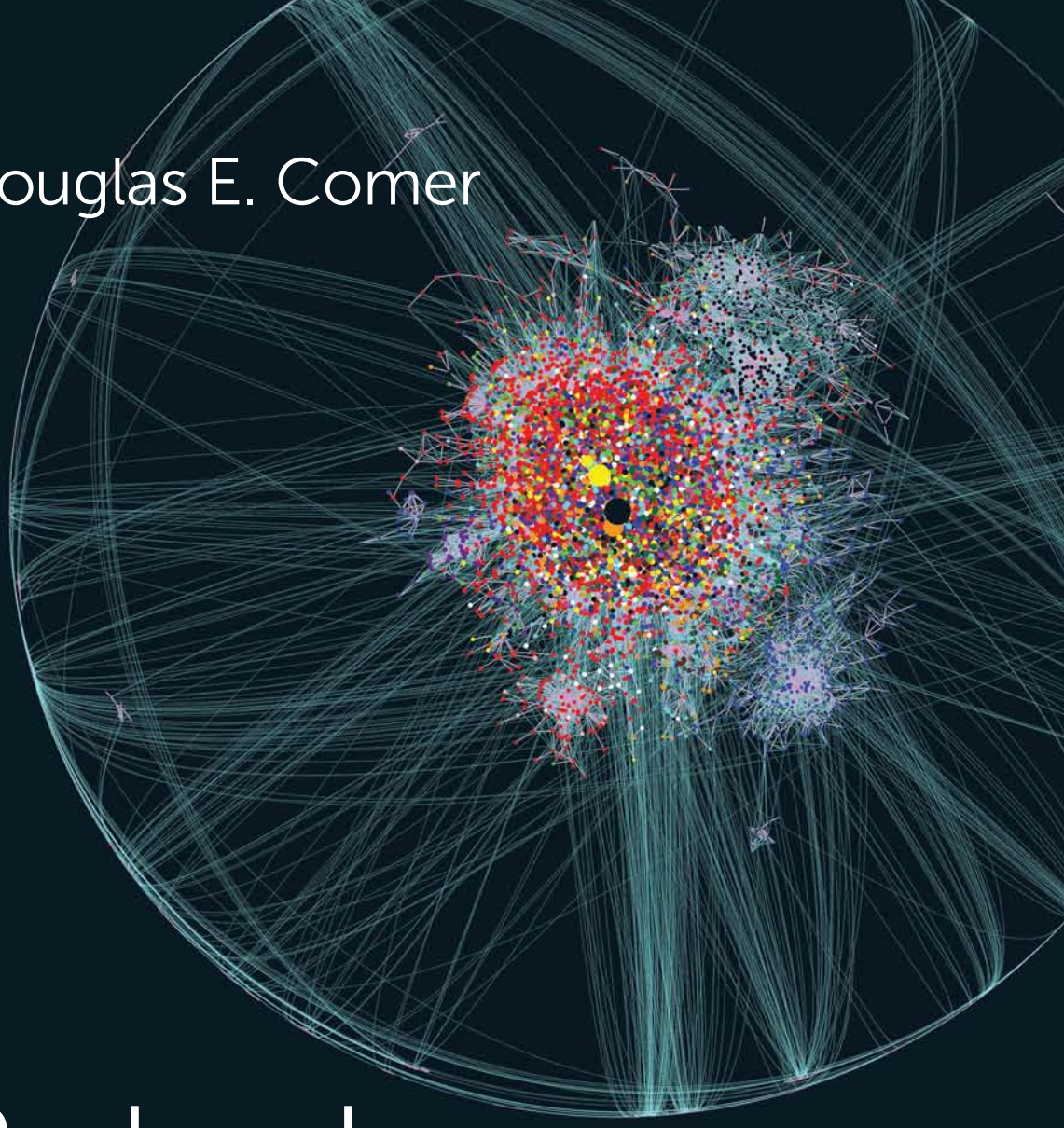
Douglas E. Comer



Redes de Computadores e Internet

bookman

6ª EDIÇÃO

O autor

Dr. Douglas Comer é um internacionalmente reconhecido especialista em redes de computadores, protocolos TCP/IP e Internet. Foi um dos pesquisadores que contribuíram com a formação da Internet no fim dos anos 1970 e nos anos 1980, sendo membro do *Internet Architecture Board*, o grupo responsável por guiar o desenvolvimento da Internet. Também foi presidente do comitê técnico CSNET, membro do comitê executivo CSNET e presidente do Distributed Systems Architecture Board da DARPA (*Defense Advanced Research Projects Agency*). Foi ainda Vice-Presidente de Pesquisa na Cisco Systems.

Comer é consultor de projeto de redes de computadores para empresas e palestrante frequente em ambientes acadêmicos e profissionais ao redor do mundo. Seu sistema operacional, Xinu, e a implementação de protocolos TCP/IP (ambos documentados em seus livros) são utilizados em produtos comerciais. É professor honorário de Ciências da Computação na Purdue University, onde leciona redes de computadores, redes de internet, arquitetura de computadores e sistemas operacionais. Lá desenvolveu laboratórios de informática inovadores que dão aos alunos a oportunidade de ter experiências práticas na operação de sistemas, redes de computadores e protocolos.

Além de escrever livros técnicos *best-sellers*, já traduzidos para 16 idiomas, atuou como editor norte-americano do periódico *Software – Practice and Experience* por 20 anos. Comer é membro da ACM. Informações adicionais podem ser encontradas em: *www.cs.purdue.edu/homes/comer.*

C732r Comer, Douglas E.
Redes de computadores e internet [recurso eletrônico] / Douglas E. Comer ; tradução: José Valdeni de Lima, Valter Roesler. – 6. ed. – Porto Alegre : Bookman, 2016.

Editado como livro impresso em 2016.
ISBN 978-85-8260-373-4

1. Redes de computadores. 2. Internet. I. Título.

CDU 004.7

Catalogação na publicação: Poliana Sanchez de Araujo – CRB 10/2094

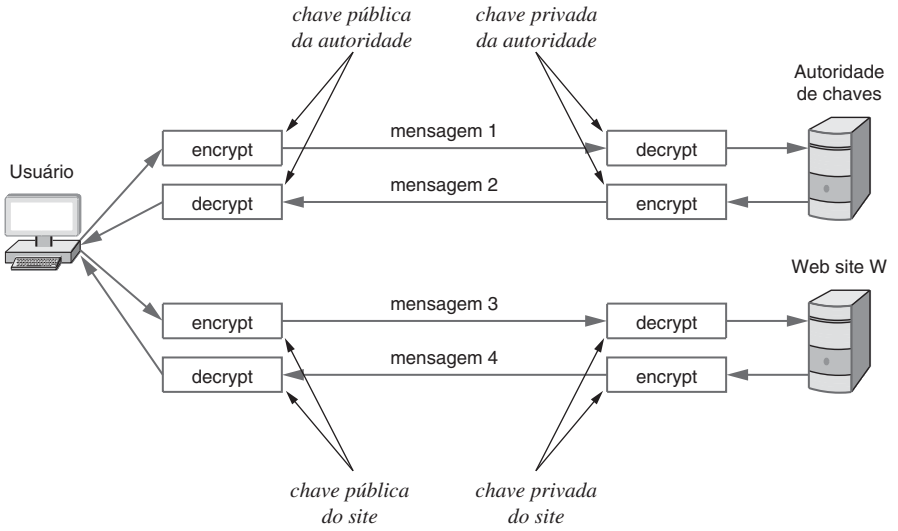


Figura 29.7 Ilustração da utilização de uma autoridade de chaves para obter uma chave pública.

29.13 Firewalls

Embora a criptografia ajude a resolver muitos problemas de segurança, uma segunda tecnologia é necessária. Conhecida como *firewall de Internet*[3], essa tecnologia ajuda a proteger a rede e os computadores da organização de tráfego indesejado. Da mesma forma que uma parede corta-fogo (firewall) convencional, um firewall de Internet é projetado para evitar que os problemas da Internet atinjam os computadores de uma organização.

Um firewall é colocado entre uma organização e o resto da Internet, e todos os pacotes que entram ou saem da organização passam por ele. A Figura 29.8 ilustra a arquitetura.

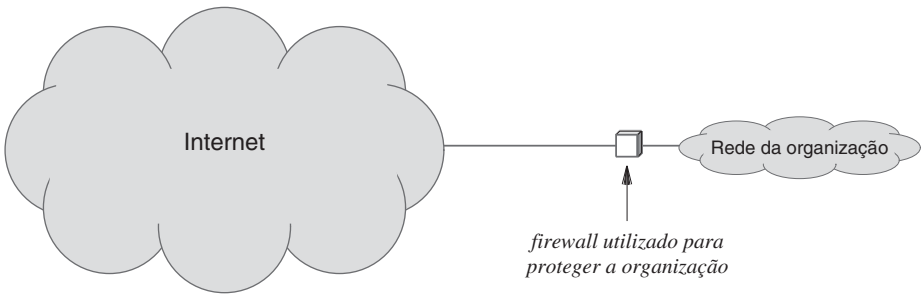


Figura 29.8 Ilustração de um firewall no caminho entre a Internet e uma intranet da organização.

[3] O termo é derivado do conceito de parede corta-fogo, que se constitui num obstáculo físico à prova de fogo entre duas partes de uma estrutura e visa impedir que o fogo passe para o outro lado.

Se uma organização tiver várias conexões com a Internet, um firewall deve ser colocado em cada uma delas, e todos os firewalls da organização devem ser configurados para cumprir a sua política de segurança. Além disso, o próprio firewall deve ser protegido contra a falsificação. Para resumir:

- Todo o tráfego que entra na organização passa pelo firewall.
- Todo o tráfego que sai da organização passa pelo firewall.
- O firewall implementa a política de segurança e descarta pacotes que não aderem a ela.
- O firewall em si é imune a ataques de segurança.

O firewall é a ferramenta de segurança mais importante usada para manipular a conexão entre duas organizações que não confiam uma na outra. Ao colocar um firewall em cada conexão de rede externa, uma organização pode definir um *perímetro de segurança* que impede que pessoas de fora interfiram nos computadores internos a esse perímetro. Em particular, um firewall pode impedir que pessoas externas descubram os endereços dos computadores da organização, inundem as suas redes com tráfego indesejado, ou ataquem um computador por meio do envio de uma sequência de datagramas IP que visam uma falha. Além disso, um firewall pode impedir a exportação de dados indesejados (por exemplo, um usuário na organização inadvertidamente importa um vírus que envia uma cópia do seu disco para alguém de fora da organização).

Do ponto de vista de um gerente, um firewall tem uma importante vantagem sobre outros esquemas de segurança: ele centraliza o controle e, assim, melhora a segurança de forma dramática. Para garantir a segurança sem um firewall, uma organização deve tornar cada um dos seus computadores seguro. Além disso, cada computador tem de aplicar as mesmas políticas. O custo de contratação de pessoal para administrar muitos computadores é alto, e uma organização não pode depender de usuários individuais para configurar seus computadores corretamente. Com um firewall, um gerente pode restringir todo o tráfego de Internet a um pequeno conjunto de computadores e usar a equipe para configurar e monitorar esse conjunto. No caso extremo, todo acesso externo pode ser restrito a um único computador. Assim, um firewall permite a uma organização economizar dinheiro e garantir mais segurança.

29.14 Implementação de firewall com filtro de pacotes

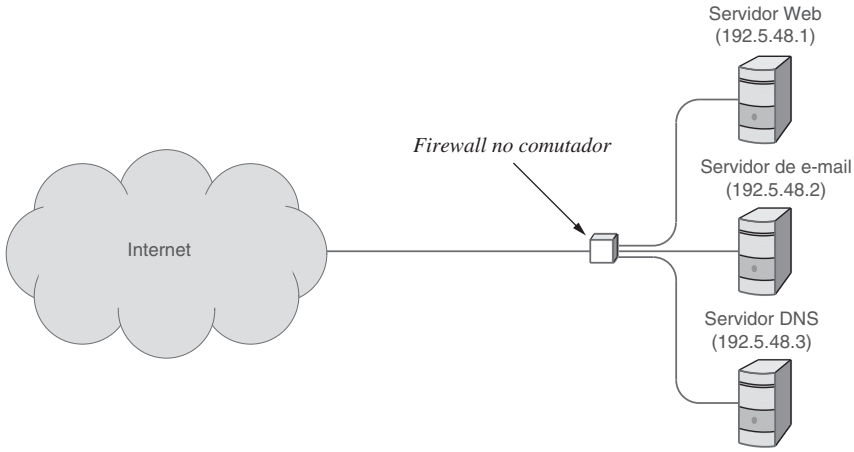
Embora o firewall possa ser um dispositivo independente, a maioria deles é incorporada em um comutador ou em um roteador. Em ambos os casos, o mecanismo usado para construir o firewall é conhecido como *filtro de pacotes*. Um filtro consiste em um mecanismo configurável que examina os campos em cada cabeçalho de pacote e decide se deve permitir que ele passe pelo roteador ou seja descartado. Um gerente configura o filtro de pacotes especificando quais tipos de pacotes podem passar em cada sentido (é mais seguro especificar os tipos de pacotes permitidos em vez dos que devem ser descartados).

Para o TCP/IP, uma especificação de filtro de pacotes geralmente inclui um tipo de quadro (0x0800 para o IPv4 e 0x08DD para o IPv6), um *endereço de origem* ou um *endereço de destino* IP (ou ambos), um tipo de datagrama e um número de porta. Por exemplo, para permitir que pessoas de fora acessem o servidor Web da organização, um filtro de pacotes pode permitir todos os quadros de entrada que contenham um datagra-

ma IP carregando TCP a partir de qualquer endereço e porta de origem com destino à porta 80 e um endereço IP de destino igual ao endereço IP do servidor Web.

Como permite a um gerente especificar combinações de endereços e serviços de origem e destino, o filtro de pacotes em um firewall possibilita que ele controle o acesso a serviços específicos em computadores específicos. Por exemplo, um gerente pode optar por permitir que o tráfego de entrada acesse um servidor Web em um computador, um servidor de e-mail em outro e um servidor DNS em um terceiro. É claro que um gerente também deve instalar regras de firewall para permitir o tráfego dos pacotes de resposta a partir do site. A Figura 29.9 ilustra uma configuração de firewall para tal site.

A habilidade de seletivamente permitir pacotes para um determinado serviço permite ao gerente controlar de modo cuidadoso os serviços que são visíveis externamente. Assim, mesmo se um usuário inadvertidamente (ou intencionalmente) inicia um servidor de e-mail em seu computador, pessoas externas à rede não serão capazes de entrar em contato com esse servidor.



Dir	Tipo de quadro	IP de origem	IP de destino	Tipo	Porta de origem	Porta de destino
In	0x0800	*	192.5.48.1	TCP	*	80
In	0x0800	*	192.5.48.2	TCP	*	25
In	0x0800	*	192.5.48.3	TCP	*	53
In	0x0800	*	192.5.48.3	UDP	*	53
Out	0x0800	192.5.48.1	*	TCP	80	*
Out	0x0800	192.5.48.2	*	TCP	25	*
Out	0x0800	192.5.48.3	*	TCP	53	*
Out	0x0800	192.5.48.3	*	UDP	53	*

Figura 29.9 Exemplo de configuração de firewall para um site com três servidores que executam o IPv4. Os asteriscos são usados para denotar entradas que aceitam qualquer valor.

Podemos resumir:

> *Um firewall utiliza o filtro de pacotes para impedir a comunicação indesejada. Cada especificação do filtro gera uma combinação de campos de cabeçalho, incluindo endereços IP de origem e destino, números de porta, bem como o tipo do protocolo de transporte.*

29.15 Sistemas de detecção de intrusão

Um *sistema de detecção de intrusão* (IDS, *Intrusion Detection System*) monitora todos os pacotes que chegam a um site e notifica o administrador do site se uma violação de segurança é detectada. Um IDS fornece uma camada extra de segurança – mesmo que um firewall impeça um ataque, um IDS pode notificar o administrador do site que o problema está ocorrendo.

A maioria dos IDSs pode ser configurada para observar tipos específicos de ataques. Por exemplo, um IDS pode ser configurado para detectar ataques de *varredura de portas* (*port scanning*) em que um atacante envia datagramas UDP ou tenta abrir uma conexão TCP em sucessivas portas do servidor. Da mesma forma, um IDS pode ser configurado para detectar um potencial ataque de *inundação de SYN* (*SYN flooding*), observando se acontecem repetidos pacotes SYN de uma determinada fonte. Em alguns casos, o IDS e o firewall são interligados para fornecer filtragem automática: em vez de apenas notificar o administrador do site sobre um problema, o IDS cria uma regra de firewall que bloqueia os pacotes que estão causando-o. Por exemplo, se o IDS detectar uma inundação SYN proveniente de uma determinada origem, ele pode instalar uma regra de firewall que bloqueia pacotes a partir dessa origem. A razão para usar uma abordagem automatizada é a velocidade – um ser humano leva muitos segundos para responder após ter sido notificado sobre um problema e, em uma rede gigabit, mais de 50 mil pacotes podem chegar por segundo. Assim, uma resposta rápida é necessária para minimizar o impacto de um problema.

A principal diferença entre um IDS e um firewall é que aquele inclui *informações de estado*, ao contrário deste, que aplica as regras para um único pacote de cada vez. Assim, um IDS pode manter um histórico de pacotes. Por exemplo, apesar de um firewall determinar se pode ou não admitir um determinado pacote SYN, um IDS pode observar que muitos SYNs estão chegando de uma única fonte. É claro que o IDS exige mais cálculos e acesso à memória do que um firewall, não conseguindo lidar com tantos pacotes por segundo.

29.16 Varredura de conteúdo e inspeção detalhada de pacotes

Embora possa lidar com muitos problemas de segurança, um firewall tem uma limitação grave: só examina campos no cabeçalho do pacote, não tendo condições de verificar os dados úteis dele. Para entender por que o conteúdo dos pacotes pode ser importante, considere um vírus de computador. Uma das formas mais comuns de vírus é introduzida numa organização por meio de um anexo de e-mail; o invasor envia uma mensagem de e-mail com um programa de computador como um anexo. Se um usuário desavisado

abre o anexo, o programa pode instalar um software malicioso no computador dele, incluindo *malwares*[4], tais como um vírus.

De que forma um site pode evitar problemas como a instalação de um vírus? A resposta reside na *análise do conteúdo* dos pacotes. Existem dois tipos de análise de conteúdo:

- Varredura de arquivo (*file scanning*)
- Inspeção detalhada de pacotes (DPI, *Deep Packet Inspection*)

Varredura de arquivo (file scanning). A abordagem mais simples para analisar o conteúdo trabalha com arquivos inteiros. A varredura de arquivos é uma técnica bastante conhecida usada pelo software de segurança instalado em um PC típico. Em essência, um scanner de arquivo recebe o arquivo como entrada e procura padrões de bytes que indicam um problema. Por exemplo, muitos scanners de vírus procuram sequências de bytes conhecidas como *impressões digitais* (*fingerprints*). Assim, uma empresa que vende um antivírus recolhe cópias de vírus, coloca cada uma em um arquivo, encontra sequências de bytes que são incomuns e cria uma lista de todas as sequências. Quando um usuário executa o software antivírus, este varre os arquivos do disco do usuário procurando algum que contenha as sequências de bytes que correspondem aos vírus da lista. A varredura de arquivos funciona bem para identificar os problemas mais comuns. É claro que a varredura pode produzir *falsos positivos* se um arquivo legítimo contiver uma sequência da lista, e pode produzir *falsos negativos* se existir um novo vírus cuja sequência não está na lista.

*Inspeção detalhada de pacotes (*DPI, *Deep Packet Inspection).* A segunda forma de análise de conteúdo opera em pacotes, e não em arquivos. Isto é, em vez de meramente examinar os cabeçalhos de pacotes que passam para o local, um mecanismo de DPI também examina os dados da carga útil do pacote. Note que a DPI não exclui o exame do cabeçalho – em muitos casos, o conteúdo dos dados não pode ser interpretado sem que se examinem os campos no cabeçalho do pacote.

Como um exemplo de DPI, considere um ataque em que um pequeno erro de ortografia de um nome de domínio é usado para enganar o usuário. Uma organização que quer impedir tais ataques pode criar uma *lista negra*, ou seja, um conjunto de URLs que são conhecidas por apresentarem riscos à segurança. Para acessar a lista, cada usuário do site deve configurar seu navegador para utilizar um *proxy Web* (ou seja, um sistema Web intermediário que verifica a URL antes de buscar a página solicitada). Como alternativa, um filtro de DPI pode ser configurado para inspecionar cada pacote de saída e observar se há alguma solicitação HTTP para qualquer um dos sites na lista negra.

A principal desvantagem da DPI é a sobrecarga computacional. Como a carga útil do pacote em um quadro Ethernet pode ser mais de vinte vezes maior do que o cabeçalho, a DPI pode exigir vinte vezes mais processamento do que a simples inspeção do cabeçalho. Além disso, o payload do pacote não é dividido em campos fixos como o cabeçalho, o que significa que os mecanismos de DPI devem analisar dinamicamente os conteúdos durante uma inspeção. Assim:

> *Como examinam os dados úteis dos pacotes, que são muito maiores do que os seus cabeçalhos e não são organizados em campos fixos, mecanismos de DPI estão limitados a redes de baixa velocidade.*

[4] Softwares maliciosos.

29.17 Redes privadas virtuais (VPNs)

Uma das tecnologias mais importantes e amplamente utilizadas em segurança usa criptografia para fornecer acesso seguro à intranet da organização a partir de um local remoto, usando protocolos padrão sobre a Internet não segura. Conhecida como *redes privadas virtuais* (VPNs, *Virtual Private Networks*), a tecnologia foi originalmente concebida para proporcionar uma interligação de baixo custo entre os vários locais geográficos de uma organização. Para entender a motivação, considere as seguintes alternativas de interconexão:

- *Conexões em redes privadas.* Uma organização aluga circuitos de dados para ligar os seus sites. Cada conexão interliga um roteador em um dos locais da organização com um roteador em outro local; dados passam diretamente de um roteador para o outro.
- *Conexões na Internet pública.* Cada site contrata com um ISP local para o serviço de Internet. Os dados enviados de um site corporativo para outro passam através da Internet.

A Figura 29.10 ilustra as duas possibilidades aplicadas a uma organização com três sites.

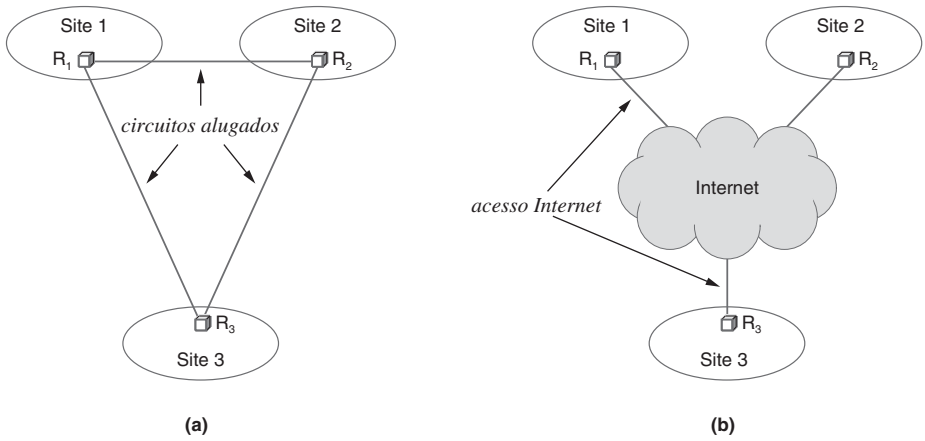


Figura 29.10 Sites ligados por (a) circuitos alugados e (b) Internet.

A principal vantagem do uso de circuitos privados para interligar os locais é que a rede resultante fornece mais garantias de que os dados permaneçam confidenciais[5]. As empresas de telefonia garantem que nenhuma outra organização tenha acesso a um circuito alugado, o que significa que nenhuma outra organização pode ler os dados que passam de um site para outro. A principal vantagem do uso de conexões de Internet é o baixo custo – em vez de pagar por circuitos dedicados para conectar sites, a organização só precisa pagar pelo serviço de Internet em cada local. Infelizmente, a

[5] A rigor, o termo *privado* é um equívoco; no entanto, os profissionais de redes costumam usar a palavra *privado* com o sentido de *confidencial*.

Internet não pode garantir a confidencialidade. Como viaja da origem para o destino, um datagrama passa através de redes intermediárias que podem ser compartilhadas; como consequência, outras empresas poderão obter cópias do datagrama e examinar seu conteúdo.

Uma VPN combina o melhor de ambas as abordagens, usando a Internet para transferir dados entre os locais e tomando medidas adicionais para garantir que os dados não possam ser acessados por pessoas externas. Assim, em substituição a um circuito alugado caro, uma VPN usa criptografia – todos os pacotes enviados entre os sites de uma organização são criptografados antes de serem enviados.

Para tornar a VPN ainda mais protegida dos ataques, uma organização pode dedicar roteadores à função VPN e usar um firewall para proibir os roteadores VPN de aceitar quaisquer pacotes não autorizados. Por exemplo, suponha que cada um dos roteadores na Figura 29.10 (b) são dedicados à função VPN (ou seja, suponha que o site tenha roteadores adicionais que lidam com o tráfego normal da Internet). Um firewall que protege o roteador VPN no Site 1 pode restringir todos os pacotes de entrada para ter um endereço IP de origem do roteador VPN no Site 2 ou o roteador VPN no Site 3. Da mesma forma, um firewall em cada um dos outros dois locais restringe os pacotes de entrada nesse site. As restrições ajudam a tornar o sistema resultante mais imune à falsificação de endereço e a ataques DoS.

29.18 O uso da tecnologia VPN para o teletrabalho

Embora originalmente concebida para interligar sites, a tecnologia VPN tornou-se extremamente popular entre os funcionários que fazem *teletrabalho* (ou seja, que trabalham a partir de um local remoto). Há duas formas de VPN:

- Dispositivo autônomo
- Software de VPN

Dispositivo autônomo. A organização disponibiliza para o funcionário um dispositivo físico que às vezes é chamado de *roteador VPN*. O dispositivo se conecta à Internet e estabelece automaticamente uma comunicação segura para um servidor VPN no site da organização, fornecendo conexões de rede local para o usuário conectar computadores e telefones IP. Logicamente, o dispositivo VPN estende a rede da organização para o site do usuário, permitindo que os computadores conectados ao dispositivo VPN operem como se estivessem conectados à rede corporativa. Assim, quando o computador do usuário inicializa e obtém um endereço IP, o endereço é emitido pelo servidor DHCP da organização. Da mesma forma, a tabela de encaminhamento no computador do usuário é configurada como se o computador estivesse localizado no site da organização – sempre que o computador envia um pacote, o dispositivo VPN criptografa-o e envia a versão criptografada através da Internet para a organização. Sempre que um pacote chega da organização, o dispositivo VPN descriptografa-o e transmite o resultado para o computador do usuário.

Software de VPN. Embora um dispositivo autônomo funcione bem para um funcionário que trabalha em casa ou em um escritório remoto, adequado para funcionários que viajam. Para lidar com esses casos, uma organização usa um *software de VPN* que é executado no computador pessoal do usuário. Um usuário conecta-se à Internet e, em

seguida, inicia o aplicativo VPN. Quando inicializa, a aplicação VPN insere-se como intermediária na comunicação com a Internet; assim, o software VPN criptografa cada pacote de saída, envia o pacote criptografado para o servidor VPN corporativo e descriptografa cada pacote de entrada.

29.19 Tunelamento versus criptografia de pacotes

A discussão a respeito de VPNs levanta uma questão interessante: como os dados devem ser criptografados para serem transmitidos através da Internet? Existem três opções principais:

- Criptografia da carga útil (payload)
- Tunelamento IP-em-IP
- Tunelamento IP-em-TCP

Criptografia da carga útil (payload). Para manter o conteúdo de um datagrama confidencial, a *criptografia de payload* criptografa os dados úteis de um datagrama, mas deixa o cabeçalho intacto. Como os campos de cabeçalho não são criptografados, alguém que interceptar o pacote será capaz de aprender os endereços de origem e de destino utilizados, bem como os números de porta. Por exemplo, suponha que o diretor financeiro (CFO, *Chief Financial Officer*) está em um local e o presidente da empresa em outro. Suponha ainda que o CFO envia uma pequena mensagem de e-mail para o presidente sempre que o noticiário financeiro é bom, mas uma longa explicação sempre que as notícias financeiras não são boas. Uma pessoa de fora pode observar que, logo depois que flui uma mensagem curta entre dois computadores específicos, os preços das ações sobem.

Tunelamento IP-em-IP. Algumas VPNs usam a tecnologia de *tunelamento IP-em-IP* para criptografar o datagrama inteiro, incluindo o cabeçalho, quando ele passa através da Internet. O software VPN criptografa todo o datagrama, incluindo o cabeçalho, e coloca o resultado dentro de outro datagrama para a transmissão. Por exemplo, considere as conexões na Figura 29.10 (b). Suponha que o *Computador X* no *Site 1* tenha enviado um datagrama para o *Computador Y* no *Site 2*. O datagrama é encaminhado pelo Site 1 para o roteador R_1 (ou seja, o roteador que conecta o Site 1 com a Internet). A instalação da VPN em R_1 criptografa o datagrama original e o encapsula em um novo datagrama para a transmissão ao roteador R_2, que é o roteador do Site 2. Quando o datagrama encapsulado chega, o software VPN em R_2 descriptografa o payload para extrair o datagrama original e encaminha-o para o Computador Y. A Figura 29.11 ilustra o encapsulamento.

Na Figura 29.11, (a) mostra o datagrama original, (b) mostra o resultado da encriptação e (c) mostra o datagrama que é transmitido de R_1 a R_2. Note que os endereços internos estão ocultos porque todos os datagramas que viajam através da Internet entre os Sites 1 e 2 possuem os roteadores R_1 e R_2 como endereços de origem e de destino.

Para resumir:

> *Quando uma VPN usa encapsulamento IP-em-IP, todos os campos do datagrama original são criptografados, incluindo o cabeçalho original.*

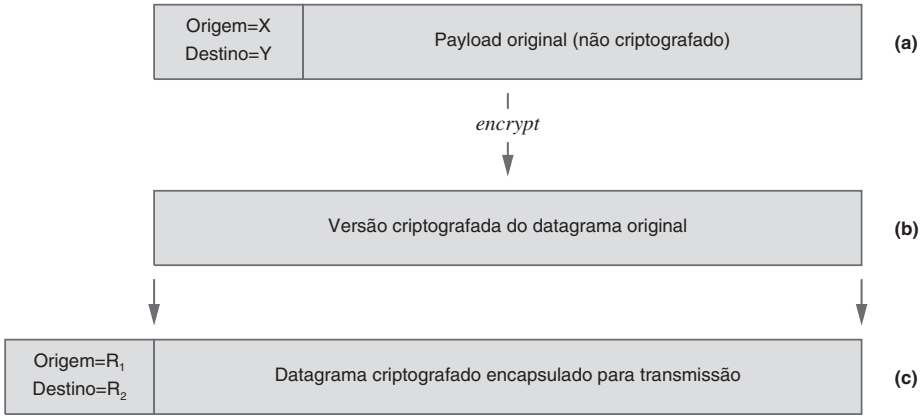


Figura 29.11 Ilustração de encapsulamento IP-em-IP usado com uma VPN.

Tunelamento IP-em-TCP. A terceira alternativa usada para manter dados confidenciais envolve a utilização de um túnel TCP, ou seja, duas partes estabelecem uma conexão TCP e depois usam-na para enviar datagramas criptografados. Quando um datagrama deve ser enviado, todo ele é criptografado, um pequeno cabeçalho é adicionado para marcar o limite entre datagramas, e o resultado é enviado através da conexão TCP. Tipicamente, o cabeçalho consiste em um número inteiro de 2 bytes que especifica o comprimento do datagrama. Na outra extremidade da ligação TCP, o software VPN receptor lê o cabeçalho e, em seguida, lê o número especificado de bytes adicionais para obter o datagrama. Uma vez que todo o texto criptografado para um datagrama tenha sido recebido, o receptor o descriptografa, obtendo o datagrama original.

A principal vantagem do uso de IP-em-TCP em vez de IP-em-IP é a garantia de entrega: o TCP garante que todos os datagramas enviados entre dois sites cheguem de forma confiável e em ordem. A principal desvantagem do uso de IP-em-TCP é o bloqueio temporário no caso de perda de pacotes: como todos os datagramas devem ser entregues em ordem, se um segmento TCP é perdido ou atrasado, o TCP não pode entregar dados de segmentos sucessivos, mesmo que eles tenham chegado corretamente. Se pensarmos que uma VPN é a transferência de uma fila de pacotes, toda a fila permanece bloqueada até que o primeiro datagrama tenha sido entregue.

Existe uma última questão relacionada ao tunelamento VPN: desempenho. Há três aspectos:

- Latência
- Taxa de transferência (throughput)
- Sobrecarga (overhead) e fragmentação

Latência. Para entender a questão da latência, considere uma organização na Costa Oeste dos Estados Unidos e assuma que um funcionário viaja para a Costa Leste, a cerca de 5 mil quilômetros de distância. Lembre-se de que o software de VPN transfere datagramas apenas até o roteador de entrada da organização – uma vez que atinge a organização, um datagrama deve ser roteado para o seu destino. Por exemplo, se o funcionário navega em uma página Web, cada requisição deve trafegar a partir da localização atual do funcionário até o servidor VPN da organização e, de lá para o servidor Web. A resposta deve trafegar de

volta para o servidor VPN da organização e, finalmente, para o empregado no local remoto. A latência necessária para acessar um recurso próximo ao funcionário é especialmente elevada, porque datagramas devem trafegar a partir do funcionário em toda a VPN até a organização na Costa Oeste e de volta para o recurso na Costa Leste. Como resultado, essas viagens de ida e volta exigem que um datagrama faça quatro travessias do continente.

Taxa de transferência (throughput). Outro problema com uma VPN convencional decorre do throughput disponível na Internet. Esse problema pode tornar-se mais relevante quando forem usados aplicativos projetados para uma LAN de alta velocidade. Em algumas organizações, por exemplo, as páginas da Web que os funcionários usam para o trabalho interno da empresa contêm muitos gráficos. A LAN no ambiente local proporciona uma taxa de transferência suficiente para fazer o download rápido das páginas Web entretanto, para um usuário remoto conectado via VPN, a baixa taxa de transferência pode tornar frustrante a espera por uma página Web.

Sobrecarga (overhead) e fragmentação. Um terceiro aspecto do desempenho surge porque o encapsulamento adiciona sobrecarga no datagrama. Para entender o problema, suponha que um site utiliza Ethernet e que o aplicativo criou um datagrama de 1.500 bytes (ou seja, o datagrama é tão grande quanto o MTU da rede). Quando um roteador VPN encapsula o datagrama criptografado em outro datagrama IP, pelo menos 20 bytes são adicionados no cabeçalho, o que faz com que o datagrama resultante exceda o MTU da rede e com que seja gerada fragmentação antes da transmissão. Como ambos os fragmentos devem chegar antes do datagrama pode ser descriptografado, a probabilidade de perda ou atraso é maior.

29.20 Tecnologias de segurança

Várias tecnologias de segurança foram criadas para serem usadas na Internet. Os destaques incluem:

- *PGP* (*Pretty Good Privacy*). Um sistema de criptografia que os aplicativos podem usar para criptografar dados antes da transmissão. O PGP foi desenvolvido no MIT e é especialmente popular entre os cientistas da computação.
- *SSH* (*Secure Shell*). Um protocolo de camada de aplicação para o login remoto que garante a confidencialidade, criptografando os dados antes da transmissão através da Internet.
- *SSL* (*Secure Socket Layer*). Uma tecnologia originalmente concebida pela Netscape Communications que usa criptografia para fornecer autenticação e confidencialidade. O software SSL fica entre a aplicação e a API de sockets e criptografa os dados antes de transmiti-los através da Internet. O SSL é usado em uma conexão Web para permitir que os usuários realizem transações financeiras com segurança (por exemplo, enviem um número de cartão de crédito para um servidor Web).
- *TLS* (*Transport Layer Security*). Projetado pelo IETF no final dos anos 1990 como um sucessor para o SSL, o TLS baseia-se na versão 3 do SSL. Tanto o SSL como o TLS estão disponíveis para uso com HTTPS.
- *HTTPS* (*HTTP Security*). Não é efetivamente uma tecnologia distinta, pois combina HTTP com SSL ou TLS e um mecanismo de certificação para fornecer aos usuários comunicação autenticada e confidencial através da Web. A HTTPS utiliza a porta TCP 443 em vez da porta 80.

- *IPsec* (*IP security*). É o padrão de segurança usado com datagramas IP. Ele utiliza técnicas de criptografia e permite ao remetente utilizar autenticação (ou seja, validar o remetente e o destinatário do datagrama) ou confidencialidade (ou seja, criptografar o payload do datagrama).
- *RADIUS (Remote Authentication Dial-In User Service)*. Um protocolo usado para fornecer autenticação centralizada, autorização e prestação de contas (accounting). O RADIUS é popular entre os ISPs, que têm usuários de conexão discada, e os sistemas de VPN, que fornecem acesso a usuários remotos.
- *WEP e WPA (Wired Equivalent Privacy e Wi-Fi Protected Access)*. O WEP foi originalmente parte do padrão de rede local sem fio Wi-Fi[6] e foi usado para manter as transmissões confidenciais. Pesquisadores da U.C. Berkeley encontraram vários pontos fracos no padrão WEP, fazendo com que o WPA (mais tarde *WPA2*) fosse desenvolvido em substituição a ele.

29.21 Resumo

As redes de computadores e a Internet podem ser utilizadas para atividades criminosas; as maiores ameaças incluem *phishing*, falsificação, golpes, negação de serviço, perda de controle e perda de dados. As técnicas utilizadas em ataques incluem: escutas telefônicas, repetição, *buffer overflow*, *spoofing* de endereço e nome, DoS com pacotes, *SYN flood*, quebra de senha, *port scanning* e interceptação de pacotes.

Cada organização precisa definir uma política de segurança que especifica aspectos como a integridade dos dados (proteção contra alterações), a disponibilidade de dados (proteção contra a interrupção do serviço), a confidencialidade de dados e a privacidade (proteção contra intromissão). Além disso, a organização deve considerar a prestação de contas (ou seja, como manter relatórios para auditoria) e a autorização (ou seja, como a responsabilidade pela informação é transmitida de uma pessoa para outra).

Um conjunto de tecnologias foi criado para fornecer diversos aspectos da segurança. O conjunto inclui: criptografia, *hashing*, assinaturas e certificados digitais, firewalls, sistemas de detecção de intrusão, inspeção detalhada de pacotes, verificação de conteúdo e redes privadas virtuais. A criptografia é uma das tecnologias mais fundamentais entre as utilizadas nos mecanismos de segurança.

A criptografia de chave privada usa uma única chave para cifrar e decifrar mensagens; o remetente e o destinatário devem manter a chave em segredo. Sistemas de criptografia de chave pública usam um par de chaves; uma chave é mantida em segredo e outra (a chave pública) é amplamente anunciada. As assinaturas digitais são obtidas pela utilização de criptografia para autenticar as mensagens. Uma autoridade de chaves pode emitir certificados para validar as chaves públicas.

Um firewall protege um site contra ataques limitando os pacotes que podem entrar ou sair. Para configurar um firewall, um gerente elabora um conjunto de regras que identificam os pacotes por meio de uma associação de valores específicos nos campos do cabeçalho. Sistemas de detecção de intrusão mantêm informações de estado e podem identificar ataques como inundação de SYNs.

[6] O WEP aplica-se a uma variedade de protocolos IEEE 802.11.

Redes privadas virtuais (VPNs) fornecem os benefícios de confidencialidade e também de baixo custo. A tecnologia VPN permite que um funcionário efetue teletrabalho, ou seja, trabalhe remotamente. Para manter as informações confidenciais, um remetente pode criptografar somente a carga útil do pacote (payload), usar tunelamento IP-em-IP, ou usar tunelamento IP-em-TCP. O tunelamento tem a vantagem de criptografar os cabeçalhos dos pacotes, bem como a carga útil deles. Alguns aplicativos não funcionam bem por meio de VPN, porque ela gera mais atraso, menor throughput e maior sobrecarga do que uma conexão direta.

Existem muitas tecnologias de segurança, como: PGP, SSH, SSL, TLS, HTTPS, IPsec, RADIUS e WPA.

Exercícios

29.1 Liste os principais problemas de segurança na Internet e faça uma breve descrição de cada um.

29.2 Cite uma técnica utilizada em ataques de segurança.

29.3 Suponha que um atacante encontre uma maneira de armazenar uma associação falsa no seu servidor DNS local. Como ele pode usar essa fraqueza para obter informações de sua conta bancária?

29.4 Ataques DoS costumam enviar segmentos TCP SYN. Um atacante poderia criar também um ataque de negação de serviço por meio do envio de segmentos de dados TCP? Explique.

29.5 Se uma senha contém oito letras maiúsculas e minúsculas, quantas senhas um invasor precisaria tentar para obter acesso?

29.6 Por que é difícil obter uma política de segurança de redes?

29.7 Suponha que uma empresa crie uma política de segurança especificando que somente o pessoal do RH está autorizado a ver os arquivos da folha de pagamento. Que tipo de mecanismo é necessário para implementar essa política? Explique.

29.8 Liste e descreva as oito técnicas básicas de segurança.

29.9 O que é uma lista de controle de acesso (ACL) e como é usada?

29.10 O termo *criptografia* se refere a quê?

29.11 Leia sobre o *padrão de criptografia DES* (*Data Encryption Standard*). Que tamanho de chave deve ser usado para dados extremamente importantes?

29.12 Suponha que seu amigo tenha uma chave pública e privada para uso com criptografia de chave pública. Ele poderia lhe enviar uma mensagem confidencial (ou seja, uma mensagem que só você pode ler)? Por quê?

29.13 Se você e seu amigo possuem um par de chaves públicas e privadas para um sistema de criptografia de chave pública, como é possível efetuar uma comunicação diária sem serem enganados por um ataque de repetição?

29.14 Como duas entidades podem usar a criptografia de chave pública para assinar um contrato que é então enviado para um terceiro?

29.15 O que é um certificado digital?

29.16 O que é um firewall e onde é instalado?

29.17 Muitos produtos de firewall comerciais permitem a um gerente especificar pacotes para *negar* e pacotes para *aceitar*. Qual é a desvantagem de uma configuração que só permite a negação?

29.18 Reescreva a configuração de firewall da Figura 29.9 para permitir a alguém externo efetuar *ping* em cada um dos três servidores.

29.19 Reescreva a configuração de firewall na Figura 29.9 para mover o servidor de e-mail para o computador que executa o servidor Web.

29.20 Leia sobre sistemas IDS comerciais e faça uma lista de ataques que tais sistemas podem detectar.

29.21 Considere um sistema de DPI que procura por uma sequência de K bytes em cada pacote. Se um pacote contém 1.486 bytes de carga útil, no pior caso, quantas comparações devem ser feitas para examinar o pacote, assumindo um algoritmo de comparação simples?

29.22 Por que a inspeção detalhada de pacotes não é utilizada em redes de maior velocidade?

29.23 Quais são os dois objetivos de um sistema VPN?

29.24 Quais são as três maneiras de uma VPN transferir dados através da Internet?

29.25 Quando uma VPN usa o tunelamento IP-em-IP, o que impede que um invasor leia o cabeçalho do datagrama original?

29.26 Em alguns sistemas de VPN, um remetente acrescenta um número aleatório de bits zero no datagrama antes de criptografar, e o receptor utiliza o campo de comprimento do datagrama para descartar os bits extras após o datagrama ter sido descriptografado. Assim, o único efeito do enchimento é tornar o comprimento do datagrama criptografado independente do comprimento da versão não criptografada. Por que o comprimento é importante?

29.27 Liste oito tecnologias de segurança utilizadas na Internet e descreva a finalidade de cada uma.

29.28 Leia sobre as vulnerabilidades do protocolo WEP. Como o protocolo WPA evita os problemas?

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.