Firewalls
Segurança no Controle de Acesso

Alexandre Fernandes de Moraes

Firewalls
Segurança no Controle de Acesso

1ª Edição

érica | Saraiva

Dados Internacionais de Catalogação na Publicação (CIP)
Angélica Ilacqua CRB-8/7057

Moraes, Alexandre Fernandes de
Firewalls : segurança no controle de acesso / Alexandre Fernandes de Moraes. – São Paulo : Érica, 2015.
120 p.

Bibliografia
ISBN 978-85-365-1508-3

1. Firewalls (Medidas de segurança de computadores) 2. Redes de computadores I. Título

CDD 005.98
15-0593 Editado também como livro impresso. CDU 004.056

Índices para catálogo sistemático:
1. Medidas de segurança de computadores

Copyright © 2015 da Editora Érica Ltda.

Todos os direitos reservados. Nenhuma parte desta publicação poderá ser reproduzida por qualquer meio ou forma sem prévia autorização da Editora Érica. A violação dos direitos autorais é crime estabelecido na Lei nº 9.610/98 e punido pelo Artigo 184 do Código Penal.

Coordenação Editorial:	Rosana Arruda da Silva
Capa:	Maurício S. de França
Edição de Texto:	Beatriz M. Carneiro, Paula Craveiro, Raquel F. Abranches, Silvia Campos
Produção Editorial:	Dalete Oliveira, Graziele Liborni, Laudemir Marinho dos Santos, Lívia Vilela Rosana Aparecida Alves dos Santos
Produção Digital:	Erika Amaro Rocha

O Autor e a Editora acreditam que todas as informações aqui apresentadas estão corretas e podem ser utilizadas para qualquer fim legal. Entretanto, não existe qualquer garantia, explícita ou implícita, de que o uso de tais informações conduzirá sempre ao resultado desejado. Os nomes de sites e empresas, porventura mencionados, foram utilizados apenas para ilustrar os exemplos, não tendo vínculo nenhum com o livro, não garantindo a sua existência nem divulgação. Eventuais erratas estarão disponíveis para download no site da Editora Érica.

Conteúdo adaptado ao Novo Acordo Ortográfico da Língua Portuguesa, em execução desde 1º de janeiro de 2009.

A ilustração de capa e algumas imagens de miolo foram retiradas de <www.shutterstock.com>, empresa com a qual se mantém contrato ativo na data de publicação do livro. Outras foram obtidas da Coleção MasterClips/MasterPhotos© da IMSI, 100 Rowland Way, 3rd floor Novato, CA 94945, USA, e do CorelDRAW X5 e X6, Corel Gallery e Corel Corporation Samples. Copyright© 2013 Editora Érica, Corel Corporation e seus licenciadores. Todos os direitos reservados.

Todos os esforços foram feitos para creditar devidamente os detentores dos direitos das imagens utilizadas neste livro. Eventuais omissões de crédito e copyright não são intencionais e serão devidamente solucionadas nas próximas edições, bastando que seus proprietários contatem os editores.

Seu cadastro é muito importante para nós

Ao preencher e remeter a ficha de cadastro constante no site da Editora Érica, você passará a receber informações sobre nossos lançamentos em sua área de preferência.

Conhecendo melhor os leitores e suas preferências, vamos produzir títulos que atendam suas necessidades.

Editora Érica Ltda. | Uma Empresa do Grupo Saraiva
Rua Henrique Schaumann, 270
Pinheiros – São Paulo – SP – CEP: 05413-010
Fone: (11) 3613-3000
www.editoraerica.com.br

Agradecimentos

A Deus, por sempre ter iluminado meu caminho, permitido que eu superasse minhas dificuldades e me dado a graça da abençoada família que tenho hoje.

À Editora Érica, em especial à Rosana Arruda, pela parceria de mais de 11 anos, pela oportunidade, persistência e incentivo para o lançamento deste que é o meu oitavo livro junto à Editora.

Ao meu colega e amigo Raphael Lima, pelo pensamento positivo e pela capacidade de superar os constantes desafios que vivenciamos dia após dia na HP ESP Enterprise Security Products.

À minha esposa Márcia por toda dedicação e apoio; à nossa querida princesinha Sofia e a nosso querido Augusto, que tanta alegria e amor trazem às nossas vidas.

A todos os meus alunos e ex-alunos da UNIFIEO, pela oportunidade única de aprender e compartir os conhecimentos deste livro nos últimos 10 anos.

Sobre o autor

Alexandre Fernandes de Moraes é engenheiro de computação e mestre em Segurança da Informação pela Escola Politécnica da Universidade de São Paulo (USP), pós-graduado em Administração de Empresas pela Faculdade Getulio Vargas (FGV-SP) e em Administração em Redes pelo LARC/USP.

Possui vários cursos e especializações na área de Redes e Segurança nos Estados Unidos. É profissional certificado pelo ISC2 como CISSP e CE|H pelo EC Concil.

Possui mais de 20 anos de experiência em grandes projetos de redes corporativas e em especial em segurança de redes, com atuação em projetos no Brasil, Chile, Argentina, Equador, Colômbia, Venezuela, República Dominicana, Trinidad e Tobago e México, e já palestrou em eventos de segurança dos Estados Unidos, México, Venezuela, Chile, Argentina, Uruguai, República Dominicana, Colômbia e Brasil. Desenvolveu sua experiência profissional em grandes empresas nacionais e multinacionais, como Hewlett-Packard (HP), McAfee do Brasil, Lucent Technologies e Anixter.

Atualmente é diretor técnico da HP Enterprise Security para a América Latina e docente dos cursos de graduação da UNIFIEO (Fundação Instituto de Ensino para Osasco).

É ainda autor dos livros *Redes de Computadores – Fundamentos*, *Redes de Computadores*, *Redes de Computadores – da Ethernet à Internet*, *Segurança de Redes – Fundamentos*, *Redes Sem Fio – Instalação, Configuração e Segurança – Fundamentos* e *Telemática*, publicados pela Editora Érica.

Sumário

Capítulo 1 – Conceitos de Segurança em Redes e o Papel do Firewall 13

1.1 Por que segurança? 13

1.1.1 A questão política 15

1.1.2 Cyberterrorismo 15

1.1.3 Vingança de empregados ou ex-empregados 16

1.1.4 Motivação financeira 16

1.1.5 Acesso a recursos privilegiados 17

1.2 Vulnerabilidade 17

1.2.1 Exploit 17

1.2.2 Vulnerabilidade de dia zero 18

1.2.3 Espionagem 18

1.3 Serviços de segurança 19

1.3.1 Confidencialidade 19

1.3.2 Integridade 20

1.3.3 Disponibilidade 21

1.3.4 Não repúdio 22

1.3.5 Autenticação 22

1.3.6 Autorização 23

1.3.7 Auditoria 23

1.4 O papel do firewall 24

1.4.1 Arquitetura de um ataque 25

1.4.2 Reconhecimento 25

1.4.3 Scanning/varredura 25

1.4.4 Enumeração 26

1.4.5 Exploit – exploração da vulnerabilidade 27

1.4.6 Preservação do acesso 28

Agora é com você! 28

Capítulo 2 – Firewalls 29

2.1 Firewall 29

2.2 Roteador de perímetro 31

2.3 Bastion host 31

2.4 DMZ 31

2.5 Rede externa WAN 32

2.6 Rede interna LAN 32
2.7 Filtros de pacotes 33
2.8 Stateful inspection – "verificação por contexto" 34
2.8.1 Características adicionais 35
2.9 Proxy 35
2.9.1 Proxy na camada de aplicação 37
2.9.2 Passos da política de segurança em um firewall baseado em proxy 38
2.9.3 Principais tipos de proxies 38
2.10 Firewall proxy e filtro 38
2.10.1 Análise de conteúdo 40
2.10.2 Gateway de VPN 40
2.10.3 NAT 40
2.11 IP Tables 42
2.12 Política de segurança em um firewall 43
2.13 Caso prático 44
2.13.1 Configuração IP Tables 46
2.14 Portas padrão 48
Agora é com você! 50

Capítulo 3 – Firewalls de Nova Geração – NGFW 51
3.1 O que é um Firewall de Nova Geração (NGFW)? 51
3.2 Serviço de IPS 53
3.3 Serviços avançados – Sandbox 55
3.4 Serviços avançados de reputação 56
3.5 Geolocation (localização geográfica) 57
3.6 Integração com sistemas de autenticação 57
3.7 Recursos de VPN 58
3.7.1 VPN IPSEC 58
3.7.2 VPN SSL 60
3.8 Alta disponibilidade 60
Agora é com você! 62

Capítulo 4 – Introduzindo o Microsoft ISA Server 63
4.1 O que é o Microsoft ISA Server 63
4.1.1 O que é o Kerberos? 64
4.2 Arquitetura do ISA Server 65
4.3 Regras de segurança do ISA Server 65
4.3.1 Filtro de pacote 66

4.3.2 Filtro de web 66
4.3.3 Regras de roteamento 66
4.3.4 Regras de banda....66
4.3.5 Políticas de protocolos....66
4.3.6 Regras de conteúdo e sites 66
4.4 Instalando o ISA Server 2006 para Windows 66
4.5 Monitoração 72
4.6 Configuração 73
Agora é com você!....76

Capítulo 5 – Introduzindo o Squid.... 77
5.1 O que é Squid?....77
5.2 Squid, o proxy....77
5.3 Onde nasceu o projeto do Squid? 79
5.4 O Squid como proxy transparente....82
5.5 O Squid como proxy reverso....82
5.6 HTTP_X_FORWARD_FOR 83
5.7 Instalação do Squid....83
5.8 Configuração do Squid 84
5.8.1 Definição das interfaces....84
5.8.2 Gerenciamento dos logs 86
5.8.3 Access control lists 87
5.9 Configurando o Squid para bloquear websites 87
5.10 Configurando o Squid para bloquear determinadas palavras na URL....88
5.11 Restringindo o acesso de um IP específico 89
5.12 Criando exceções para que determinadas máquinas acessem sem restrição 89
Agora é com você!....90

Capítulo 6 – Introduzindo o IP Tables.... 91
6.1 IP Tables 91
6.2 NAT (Network Address Translation) – Tradução Automática de Endereços....94
6.2.1 NAT estático 94
6.2.2 NAT dinâmico 94
6.2.3 PAT (“Port Address Translation”) 95
6.3 Como funciona o IP Tables na estrutura do Linux?....96
6.3.1 Tabela de filtragem 96
6.3.2 Tabela NAT 96
6.3.3 Tabela Mangle....96

6.4 Regras de firewall no IP Tables 96
6.5 Como instalar o IP Tables? 98
6.6 Exemplo prático 101
6.6.1 Passo a passo da configuração 102
Agora é com você! 103

Capítulo 7 – Case de Aplicação e Projeto 105
7.1 Metodologia utilizada 105
7.2 Consultoria – questionário do projeto 107
7.3 Desenvolvimento do projeto 110
7.4 Implementação das políticas 111
7.5 Testes 114
7.5.1 Regra 1 114
7.5.2 Regra 2 115
7.5.3 Regra 3 115
7.5.4 Regra 4 115
7.5.5 Regra 5 115
7.5.6 Regra 6 115
7.5.7 Regra 7 116
7.5.8 Regra 8 116
7.5.9 Regra 9 116
7.5.10 Regra 10 116
7.5.11 Regra 11 117
7.5.12 Regra 12 117
7.5.13 Regra 13 117
7.5.14 Regra 14 117
Agora é com você! 118

Bibliografia 119

Apresentação

Este livro tem como objetivo apresentar, conceituar e capacitar o leitor no uso de três importantes tecnologias de firewall do mercado, uma baseada em soluções proprietárias da Microsoft, o ISA Server, e as outras duas, o Squid e o IP Tables, em soluções de software livre.

O Capítulo 1 trata de conceitos de segurança de redes e do papel do firewall. São apresentados os pilares básicos de segurança da informação: confidencialidade, integridade e disponibilidade. Além disso, demonstra como o firewall, uma ferramenta básica de segurança, nos auxilia na implementação de políticas de segurança.

Já o Capítulo 2 conceitua a tecnologia dos firewalls. Definem-se as arquiteturas de rede em que os firewalls são implementados, bem como o seu papel no controle de acesso. São apresentadas as principais tecnologias de firewall, como o filtro de acesso (ACL), e tecnologias mais avançadas, como proxy e stateful inspection. Detalha, ainda, as características adicionais de um firewall, como a autenticação de usuários, a implementação de VPN e a filtragem de conteúdo.

O Capítulo 3 trata dos firewalls de nova geração (NGFWs). Abordam-se conceitos novos relacionados a eles e explica-se como esses firewalls permitem um controle fino no acesso a aplicações por usuários, possibilitando a inspeção e análise do tráfego proveniente do usuário, independentemente de como é feito o acesso (por tablets, dispositivos móveis, por VPN ou até mesmo por intermédio de arquitetura em Cloud).

No Capítulo 4 introduzimos o ISA Server, da Microsoft. Explicamos como instalá-lo e revisamos os seus menus de monitoração, os seus alertas e a configuração do ISA Server 2006.

No Capítulo 5 apresentamos o Squid, uma ferramenta baseada em software livre – Linux. Detalhamos o seu processo de instalação e mostramos como configurar uma política de proxy baseada no Squid. Com o passo a passo da instalação e da configuração de políticas, o Squid permitirá ao leitor expandir o seu aprendizado com a criação do seu próprio laboratório.

No Capítulo 6 introduzimos o IP Tables. Discorremos acerca de sua arquitetura e das soluções de software livre baseadas no filtro de pacotes oferecido por ele. Além disso, temos neste mesmo capítulo um passo a passo da instalação e ensinamos a monitorar os logs de segurança do IP Tables.

O Capítulo 7 apresenta um case de aplicação com um exercício prático. Montamos um cenário de rede que serve para o aluno acompanhar o passo a passo de um projeto de segurança, desde a definição de arquitetura, passando por onde instalar as paredes de firewall e concluindo com a implementação da política de segurança.

Boa leitura!

O autor

1

Conceitos de Segurança em Redes e o Papel do Firewall

Para começar

Este capítulo apresenta os principais conceitos relacionados à segurança de redes de computadores, apresentando o modelo que define a base da segurança da informação, os conceitos de perímetro e como protegê-lo, apresentando as principais ameaças a que estamos expostos na atualidade do mundo da Internet.

1.1 Por que segurança?

Sempre existe uma grande abstração quando utilizamos o termo "segurança". Isso ocorre porque, em nossas vidas, a segurança é uma das necessidades mais básicas. Afinal, precisamos nos alimentar, manter saúde, ter uma moradia e, com certeza, ter segurança para garantir tanto a nossa própria integridade física como a de nossa família.

O conceito de segurança acaba sendo subjetivo porque a percepção do que é segurança difere de pessoa para pessoa. Sendo assim, o entendimento acerca do termo pode ter uma variação muito grande. Por exemplo, até bem pouco tempo atrás, os carros nacionais não vinham com airbag nem freios ABS, ainda que ambos fossem requisitos de segurança básicos e obrigatórios em países europeus e nos Estados Unidos há mais de 20 anos. Entretanto, o motorista brasileiro sempre teve a percepção de que os veículos nacionais eram seguros, uma vez que apresentavam cintos de segurança de três pontos, que também é um item obrigatório, porém não suficiente para alcançarmos o nível de segurança adequado. Para descrever a noção de segurança que envolve o nível de

confiabilidade de um sistema, usamos, na língua inglesa, o termo "safety". Por uma questão idiomática, acabamos traduzindo para "segurança" em português.

Da mesma maneira que pensamos em segurança nos veículos, devemos pensar na segurança que é descrita pelo termo inglês "security", ou seja, a segurança relacionada a um agente externo. Nesse sentido, imagine que você precise proteger a sua casa com medidas de segurança para evitar que ela seja invadida. Erguemos muros e cercas e instalamos sistemas de proteção para evitar essa ameaça e, assim, protegermos nossas vidas. Toda vez que tratamos de uma ameaça ou um risco associado a um evento externo, usamos também o termo em português "segurança", mesmo que ele agora represente o "security".

Se desejamos proteger nossas vidas, nossa casa e nosso patrimônio de uma ameaça externa, desejamos proteger também nossas informações, nosso trabalho, nossos dados privativos, nossas informações bancárias, nossas patentes ou qualquer conteúdo intelectual. A Internet hoje pode representar uma grande ameaça à segurança dos nossos dados e à informação.

A Tecnologia da Informação conheceu um avanço fantástico nos últimos 20 anos. Praticamente todos os processos que desenvolvíamos de modo manual alguns anos atrás foram automatizados por algum sistema ou alguma aplicação. As empresas estão cada dia mais dependentes de processos de tecnologia da informação, e esse caminho não tem volta. Os computadores, smartphones e tablets são tão importantes na nossa vida e no nosso trabalho que não conseguiríamos mais ser produtivos ou trabalhar sem eles.

Toda essa tecnologia só funciona porque há processos de gestão da informação, e, sendo assim, precisamos proteger os dados que estão presentes em nossas empresas.

E quais são as ameaças?

Quando protegemos nosso patrimônio parece ser fácil identificar o inimigo. Câmeras de segurança e detectores de presença nos auxiliam nessa tarefa. No mundo digital, todavia, essa tarefa não é tão simples. Muitas vezes estamos sendo atacados, monitorados, os dados de nossas empresas estão sendo acessados e roubados e não temos a mínima ideia de que isso está acontecendo. Além disso, os processos podem estar acontecendo há dias, semanas, meses ou anos e, muitas vezes, só descobrimos quando algum terceiro nos avisa ou quando a informação privativa ou confidencial já foi vazada, podendo ser encontrada livremente em sites de redes sociais.

Quem é o nosso inimigo?

Para entender quem é o nosso inimigo devemos também entender qual a motivação que leva alguém a realizar ataques.

Até o início dos anos 2000, a maior parte dos ataques ocorridos na Internet era obra do que chamávamos de "script kids", ou seja, adolescentes e jovens talentosos que atacavam as redes com o objetivo de se divertir ou mesmo demonstrar poder e superioridade quando alcançavam seu êxito em um ataque bem-sucedido.

Era muito comum encontrarmos páginas de sites pichadas, ou seja, esses jovens simplesmente alteravam o conteúdo dessas páginas para demonstrar que haviam cumprido o desafio de atacá-las.

Embora esse comportamento representasse uma ameaça para as empresas, havia uma motivação mais inocente por trás dele, que normalmente não significava algum tipo de retorno econômico.

1.1.1 A questão política

Nos últimos anos, têm aumentando bastante os ataques direcionados a sites de governos ou mesmo os ataques contra determinadas entidades com fins políticos. Ao passo que esse fenômeno tem crescido muito nos últimos anos, o "script kid" praticamente não representa mais nenhuma ameaça, e os ataques provenientes de motivação política, o chamado "hacktivismo", está cada dia mais presente. Grupos como o "Anonymous" e o "Lulzsec" foram criados e ganharam força. São organizações de hackers que planejam e realizam ataques combinados contra agências de governos, partidos políticos e grandes empresas, como Mastercard e VISA.

Suas ações são direcionadas e normalmente buscam causar indisponibilidade por meio de ataques de negação de serviços. No Brasil, o Anonymous promoveu uma série de ataques contra sites de políticos, em especial no ano de 2014, por conta das eleições. Os hacktivistas representam uma ameaça real porque conseguem recrutar nas redes sociais um enorme número de colaboradores que são convidados a participar de seus ataques em massa.

O FBI americano e diversos mecanismos de repressão ao crime digital têm realizado pesadas investidas contra esses grupos a fim de evitar novos ataques de grandes proporções. Porém, a cada dia parece que esses grupos acabam ganhando mais força.

Rob Kints/Shutterstock.com

Figura 1.1 – Hacktivismo – máscaras usadas por integrantes do Anonymous.

1.1.2 Cyberterrorismo

Esse tipo de ameaça está se tornando mais presente a cada dia. Inclusive, o problema da segurança passou a ser considerada uma questão de Estado, principalmente para as nações desenvolvidas. Recentemente, foi noticiado pela imprensa o caso do ataque sofrido pela Sony Pictures, uma ação arrojada que impediu o lançamento de um filme parodiando o líder da Coreia do Norte, Kim Jong-un.

As agências de inteligência americanas descobriram a participação direta do governo da Coreia do Norte, e sanções contra esse país foram planejadas pelos Estados Unidos. Eis aí um exemplo do uso da tecnologia para realizar ciberataques contra Estados. Por isso, nos últimos anos a maior parte das nações vem desenvolvendo equipes de especialistas de segurança para se proteger contra esse tipo de ameaça.

Existem grupos específicos cujo objetivo é proteger a infraestrutura crítica do país, como os sistemas de tratamento de água, de geração e distribuição de energia, entre outros, contra essas ameaças.

Em 2010, um malware conhecido como Stuxnet foi injetado em uma central nuclear do Irã e atacou seu sistema SCADA (rede de instrumentação), causando uma paralisação total da central. O sistema infectou tanto a rede Microsoft como os PLCs (Programador Lógico Controlável) da planta.

O cyberterrorismo preocupa por ser a ameaça que mais cresce no mundo. Existe uma teoria que prega que as guerras do futuro serão cyberguerras, sendo realizadas diretamente pela rede. Imagine um país que tenha toda a sua comunicação via Internet bloqueada por outro país.

1.1.3 Vingança de empregados ou ex-empregados

Esse tipo de ameaça é muito perigosa. A maioria das empresas deve se preocupar, em especial em tempos de crise, com a possibilidade de vingança de empregados ou ex-empregados. Muitas vezes não tomamos os devidos cuidados com contas de acesso privilegiado, o que é um risco enorme para as empresas. Por exemplo, um funcionário mal-intencionado pode injetar um vírus na empresa, roubar dados confidenciais ou tentar apagar dados do seu banco de dados.

Há alguns anos houve uma investigação em uma fábrica de chips nos Estados Unidos. Um administrador da rede havia sido despedido recentemente, e em uma determinada manhã, quando o operador da máquina foi entrar com seu usuário e senha, um script começou a ser executado – e apagou todo o banco de dados da empresa. Após os procedimentos de investigação e perícia, descobriu-se que esse script havia sido criado pelo administrador despedido. O script verificava a data no sistema e fora programado para disparar somente no dia em que de fato disparou.

O administrador alegou que não estava mais na empresa e que não tinha mais como ter acesso aos sistemas. Porém, comprovou-se que o script por ele desenvolvido fora instalado nas máquinas antes de ele ser desligado da empresa. Esse tipo de script é o que conhecemos como “time bomb”, ou bomba-relógio.

1.1.4 Motivação financeira

O dinheiro sempre atrai o crime, e a cada dia existe mais dinheiro circulando pela rede. No Brasil da atualidade, os bancos vêm sendo as principais vítimas dessa ameaça. Milhões de reais são perdidos anualmente com fraudes eletrônicas, e nem tudo é proveniente da Internet. Porém, uma boa parte do total das perdas com essas fraudes é, sim, resultado de ação cibernética.

O problema, na maioria das vezes, não se encontra nos sistemas e servidores do banco, mas sim nos computadores dos clientes, que não tomam as devidas precauções de segurança, como instalar um antivírus e mantê-lo atualizado.

Em 2014 foi descoberta uma fraude no Brasil cujos responsáveis ficaram conhecidos como a gangue do boleto. Essa quadrilha desenvolveu um malware que, após instalado na máquina do correntista do banco, alterava a sequência de dígitos para o pagamento do boleto bancário e, dessa maneira, transferia o dinheiro do pagamento para contas de laranjas (termo usado para contas frias no nome de pessoas simples que acabam sendo enganadas pelos golpistas). A fraude pode ter rendido quase 1 bilhão de reais à quadrilha.

Esse é apenas um exemplo do interesse cada dia mais presente do crime organizado em usar a Internet como meio para cometer suas ações. Existe um estudo de mercado que revela que, hoje, o cybercrime já movimenta mais dinheiro que o tráfico de drogas.

Organismos de polícia de diversos países vêm trabalhando para criar unidades especializadas no combate a esses crimes. No Brasil, a Polícia Federal tem investindo bastante na formação de equipes e na capacitação de peritos digitais para conduzir investigações sobre o crime eletrônico.

1.1.5 Acesso a recursos privilegiados

Esse tipo de ameaça normalmente é interna e difícil de controlar. Ela ocorre quando algum usuário mal-intencionado executa alguma ferramenta de ataque, de forma a tentar explorar uma vulnerabilidade do sistema operacional para conseguir um acesso privilegiado.

Para entendermos como isso funciona, precisamos saber dois conceitos: vulnerabilidade e exploit.

1.2 Vulnerabilidade

Entende-se por vulnerabilidade uma falha de software – normalmente um bug – que, quando ocorre, deixa o sistema em um estado extremamente inseguro. Esse estado pode envolver o travamento de uma aplicação, causando indisponibilidade, o que pode expor falhas nos sistemas de controle de acesso do Kernel quando se trata de sistema operacional. O Kernel do sistema operacional é o seu coração, é ele que controla as entradas e saídas (I/O), a alocação de CPU e a alocação de memória, ou seja, todos os recursos do computador.

As vulnerabilidades do Kernel do sistema operacional são extremamente críticas porque, se forem bem exploradas, podem oferecer a usuários com recursos básicos acessos ilimitados ao sistema.

Existe um estudo que afirma que apenas 20% das vulnerabilidades são conhecidas, isto é, os outros 80% ainda não foram descobertos. Isso compreende um enorme desafio para a indústria da segurança da informação. Vale lembrar que é justamente o desconhecimento sobre essas vulnerabilidades o que nos protege contra elas. Uma vez descobertas, um enorme risco se abre.

1.2.1 Exploit

Seguindo a linha do que explicamos sobre vulnerabilidade, o exploit nada mais é do que um programa normalmente desenvolvido por hackers que será utilizado para explorar a falha de software – ou seja, a vulnerabilidade – a partir do momento em que ela se torne conhecida. Assim que

se torna publicamente conhecida, não demora muito tempo para que um hacker desenvolva um programa para explorar a vulnerabilidade.

A própria Microsoft publica toda segunda terça-feira do mês as principais vulnerabilidades que foram encontradas em seus produtos e as eventuais atualizações para corrigi-las. Oferece, assim, um prato cheio de informações para o hacker desenvolver o seu exploit e explorar sistemas que ainda não tenham a atualização aplicada.

1.2.2 Vulnerabilidade de dia zero

São conhecidas como vulnerabilidade de dia zero aquelas que ainda não são conhecidas pelos fabricantes de software. Normalmente, essas vulnerabilidades são descobertas por hackers ou investigadores independentes, e podem causar um tremendo problema na Internet. Isso ocorre porque muitas vezes essas vulnerabilidades são difundidas apenas a um pequeno grupo de hackers. Então, esse grupo cria um exploit, mas o fabricante, como não foi informado, ainda não dispõe da devida correção (patch). Os grandes ataques que ocorreram recentemente na Internet exploram vulnerabilidades de dia zero, principalmente porque a grande maioria das ferramentas de defesa, como firewalls, antivírus e sistemas IPS, ainda não possui assinaturas para bloquear tais ameaças.

Agora que já tratamos desses dois conceitos básicos fica fácil entender como um usuário consegue fazer um ataque de privilégios. Basicamente, um usuário interno sem privilégios descobre, analisando as próprias mensagens do sistema operacional, qual é a versão deste. A partir daí, busca em comunidades de hackers exploits que explorem vulnerabilidades do sistema em questão. Após executar esses exploits, os hackers conseguem muitas vezes o sucesso, ou seja, transformar uma sessão com acessos básicos em uma sessão com direitos de administração, executando assim, com sucesso, o ataque conhecido como "ataque de privilégio". De posse de uma sessão com direito de administração, o invasor está com a faca na mão para criar acessos, roubar dados e fazer uma festa na rede e nos dados da empresa.

1.2.3 Espionagem

A espionagem é uma atividade que sempre esteve presente na humanidade. Ocorre de uma maneira frenética em tempos de guerra, assim como ocorreu em grande escala nos idos da chamada "guerra fria" entre os Estados Unidos e a antiga União Soviética. Ocorre também em ambiente corporativo, em especial em empresas de alta tecnologia.

Infelizmente, é muito comum empresas mal-intencionadas contratarem espiões ou ex-agentes de organizações de inteligência, como CIA, KGB ou M-16, para atuarem comercialmente na busca de informações, segredos do negócio e invenções ainda não publicadas ou patenteadas pelas empresas.

Houve um caso clássico de espionagem na indústria de aviação. Os governos da França e da Inglaterra, nos anos 1960, iniciaram um projeto para criar o primeiro avião supersônico para uso comercial do mundo. Esse projeto ficou conhecido como Projeto Concorde. O avião apresentava um desafio muito grande de engenharia porque deveria ser rápido, mas ao mesmo tempo oferecer um voo confortável aos seus passageiros, o que não era (nem é) comum em aviões militares supersônicos.

Um dos grandes desafios do Concorde era o projeto do bico da aeronave. Vários pesquisadores renomados contribuíram em um projeto de milhares de dólares para desenhar um bico que fosse capaz de se ajustar (mudar a geometria) ao longo do voo. Vários testes foram realizados com diversos protótipos, e conseguiu-se chegar a um projeto com o desenho ideal para essa função. Todo o projeto foi custeado e desenvolvido pelo consórcio firmado entre França e Inglaterra, e a primeira aeronave comercial foi lançada em 1978.

Porém, apenas poucos meses antes do lançamento, os russos revelaram uma aeronave supersônica com o bico idêntico ao do Concorde. Como é praticamente impossível que duas equipes de engenharia isoladas desenvolvam o mesmo projeto, houve suspeita de espionagem por parte dos russos no desenvolvimento do seu Tupolev Tu-144 (era esse o nome do avião supersônico comercial russo).

Essa história é um caso clássico de espionagem industrial, que ocorre com muita frequência. Com o advento da Internet e dos meios eletrônicos, cada vez mais hackers estão sendo contratados para executar ações de espionagem. As empresas que desenvolvem produtos de alta tecnologia investem muito em processos para proteger seus segredos e invenções da ameaça de espionagem.

1.3 Serviços de segurança

Agora que já entendemos os motivos que os fazem necessários, vamos entender os principais serviços de segurança. Esses serviços nos ajudam a manter o nível de segurança adequado à informação. Envolvem basicamente três aspectos: confidencialidade, integridade e disponibilidade. Além dos básicos, existem outros serviços de segurança que envolvem aspectos como não repúdio, autenticação, autorização e auditoria.

1.3.1 Confidencialidade

A confidencialidade é o serviço de segurança que garante que apenas usuários autorizados tenham acesso à informação. Para compreendermos melhor, podemos fazer uma analogia com o envio de um envelope. Quando nele grafamos o termo "confidencial", queremos dizer que apenas as pessoas autorizadas têm acesso àquela informação, ou seja, quem criou a mensagem e o seu destinatário.

Esse serviço é um dos principais, porque basicamente todo mundo deseja manter a privacidade de suas informações, abrindo-as apenas para pessoas autorizadas, sendo a criptografia uma das ferramentas principais para esse fim. Para manter a confidencialidade, precisamos acima de tudo implementar ferramentas e mecanismos de proteção dos dados, como a criptografia.

A criptografia é uma ciência matemática que nos oferece mecanismos para proteger mensagens por meio da cifragem, um processo conhecido como encriptação. Encriptar consiste em transformar um texto claro em um texto cifrado. Apenas as pessoas autorizadas, quando de posse de uma chave criptográfica, têm acesso à informação contida no texto.

O mecanismo criptográfico faz uso de algoritmos criptográficos extremamente seguros, capazes de cifrar textos que levariam anos para ser decifrados. Alguns algoritmos com chaves grandes podem levar alguns milhares de anos até serem decifrados.

Podemos dizer que a criptografia é como um cadeado com o qual trancamos os dados, que só podem ser liberados mediante o uso de uma chave que apenas as pessoas autorizadas possuem.

musicman/Shutterstock.com

Figura 1.2 – Símbolo de criptografia.

1.3.2 Integridade

A integridade é o serviço de segurança que garante que a informação não será alterada, intencionalmente ou não, durante seu armazenamento ou processamento. Garantir a integridade é uma tarefa fundamental.

Quando realizamos uma transação computacional devemos garantir sempre que o banco de dados se mantenha íntegro. No caso de uma falha, devem existir processos que garantam o "roll back", ou seja, devemos garantir que o banco de dados sempre retorne a um ponto de integridade.

Quando falamos em dados armazenados, novamente a integridade é fundamental. Por exemplo, um sistema de backup deve garantir que os dados armazenados estão íntegros, ou seja, quando houver a necessidade de recuperá-los, devem ser recuperados da mesma maneira como foram armazenados, sem sofrer nenhum tipo de alteração.

Um exemplo de integridade em operações: quando fazemos uma transferência bancária da conta-corrente A, no valor de R$ 100,00, para uma conta-corrente B, devemos ter um controle de integridade que garanta que não ocorra um erro na transação. Isto é, não pode ocorrer o débito em uma conta sem o crédito na outra. Tampouco pode haver um crédito de R$ 1.000,00 em vez dos R$ 100,00. Essas falhas de integridade são difíceis de ocorrer, mas eventualmente acontecem. Os bancos possuem controles para detectá-las, e assim podem corrigi-las rapidamente.

Os controles de integridade podem ser implementados por meio de algoritmos de hashing. Esses algoritmos verificam se houve mudanças não previstas no armazenamento da mensagem ou na sua transmissão.

O hashing é uma sequência de caracteres de tamanho fixo, normalmente 128 ou 160 bits. É calculado segundo um algoritmo matemático e enviado ou armazenado junto com a informação. Para a verificação da integridade, o que fazemos é calcular novamente o hashing da informação restaurada do armazenamento ou recebida na comunicação e compará-lo com o hashing previamente calculado. Se forem os mesmos, não houve falha de integridade na mensagem; se, por outro lado, os resultados não baterem, a mensagem foi alterada por alguma falha no armazenamento ou na transmissão.

Os algoritmos de hashing nos auxiliam a detectar erros, porém não impedem que alguém possa intencionalmente alterar a informação. Isso ocorre principalmente porque as mensagens ficam

armazenadas de forma clara e os algoritmos de hashing são conhecidos, o que não impediria que um invasor alterasse a informação e a armazenasse novamente, recalculando o hashing da forma correta. Para esse cenário seria necessária a criptografia.

1.3.3 Disponibilidade

A disponibilidade é um dos serviços de segurança mais importantes. Se imaginarmos que, hoje, a maior parte das empresas não vive sem rede e sem os seus principais aplicativos, garantir a disponibilidade é fundamental.

Atualmente, esse serviço é um dos mais difíceis de se garantir. Nos últimos anos, temos ouvido na mídia internacional vários ataques de Negação de Serviço, os famosos DoS (Denial of Service), e de Negação de Serviços Distribuídos, DDoS (Distributed Denial of Services). O objetivo desses ataques é tornar um determinado serviço indisponível.

Basicamente, os hackers infectam inicialmente milhares de computadores na Internet criando uma rede de zoombies conhecida como BoTNet. Esses computadores podem ser controlados e acessados remotamente pelas máquinas dos hackers. Hoje, existe uma série de BotNets na Internet, e uma das redes mais conhecidas é a Zeus, que tem milhares de computadores infectados conectados a ela. Os hackers que controlam essas BotNets normalmente vendem serviços de uso da rede para realizar ataques, armazenar conteúdo e enviar spams.

No controle de uma BotNet, um hacker pode facilmente disparar um ataque de Negação de Serviços Distribuídos (DDoS) enviando um comando para que todas as milhares de máquinas acessem, com o número máximo de conexões possível, alguma máquina-alvo do ataque, normalmente um servidor de alguma corporação.

A quantidade de acessos é tão grande que o servidor não consegue responder ao enorme número de requisições, gerando dessa maneira a indisponibilidade do serviço para usuários legítimos que queiram utilizar a aplicação.

Ataques dessa magnitude são realizados também por hacktivistas, como o grupo Anonymous, e envolvem principalmente governos contra os quais eles queiram protestar.

Para bloquear esses ataques à disponibilidade existem algumas soluções. Pode-se criar uma infraestrutura mais robusta que consiga absorver o aumento de tráfego gerado pelos ataques, mas essa opção acaba sendo a mais cara, uma vez que a empresa precisa investir em links de comunicação, servidores, memória e storage em uma proporção muito maior do que realmente necessita. Essa solução envolve também uma série de outras contingências, como servidores e infraestrutura de backup.

Outra solução é usar equipamentos que identificam fluxos de dados maliciosos e os desviam via roteamento de rede, impedindo assim que a infraestrutura se torne indisponível.

A terceira e última solução é utilizar um serviço em nuvem (cloud). Nesse caso, todas as requisições de conexão são encaminhadas a esse serviço, que por sua vez reencaminha para a empresa apenas as conexões legítimas, absorvendo o excedente malicioso.

A disponibilidade não deve ser tratada apenas no âmbito desse tipo de ataque, mas também porque falhas no hardware podem ocorrer. Por exemplo, um disco, que é um dispositivo mecânico, pode

apresentar falhas. Nesse caso, precisamos utilizar uma contingência no armazenamento, que pode ser implementada por meio do uso da tecnologia RAID (Redundant Array of Inexpensive Disk).

O RAID permite que se aumente tanto a disponibilidade, por conta da redundância de discos, como a performance no acesso. Basicamente, funciona assim: quando gravamos uma informação, ela é gravada em vários discos ao mesmo tempo, assim, se um dos discos falhar, a informação estará garantida no outro. Existem vários níveis de RAID: 0, 1, 2, 3, 4, 5, 6... cada um com a sua particularidade e com o objetivo de aumentar a performance no acesso e a disponibilidade.

Além da redundância de disco podemos também criar clusters de servidores. Os clusters são infraestruturas duplicadas que permitem que, caso o equipamento principal falhe, o backup assuma. O interessante dos clusters é que eles podem trabalhar tanto no modo Ativo-Ativo como no modo Ativo-Passivo. No modo Ativo-Ativo as duas máquinas funcionam juntas, o que garante também um aumento de performance. Quando há um problema em uma delas, a outra máquina assume a carga de trabalho. Já no modo Ativo-Passivo a segunda máquina fica em stand-by, ou seja, aguardando que ocorra um problema na máquina principal. Quando o problema ocorre, ela assume a carga de trabalho.

Além da redundância de máquinas, empresas de grande porte têm soluções de data center backup. Caso haja um incidente que afete um data center, como queda de comunicação ou incêndio, o data center backup, que normalmente está localizado fisicamente a mais de trinta quilômetros do data center original, pode assumir a carga de trabalho.

A disponibilidade é sempre um dos serviços mais caros para se garantir. Porém, imagine uma bolsa de valores como a Bovespa, em que todas as transações são realizadas on-line. Se o sistema da bolsa cair e ficar fora do ar, o prejuízo será gigantesco, uma vez que as transações de compra e venda de ações não poderão ocorrer.

1.3.4 Não repúdio

O não repúdio é um serviço de segurança que consiste em técnicas e métodos que assegurem que o remetente de uma mensagem não possa negar, no futuro, o envio dela. Também é utilizado pelos sistemas de Internet Banking, providenciando mecanismos que garantam que os usuários não possam negar, *a posteriori*, uma operação realizada com sucesso anteriormente.

Esse serviço basicamente consiste em analisar os logs das transações e coletar evidências que comprovem que foi mesmo aquele determinado usuário que realizou determinada operação. Se ele tentar negar, os registros mostraram que não está falando a verdade. O não repúdio é muito utilizado também por equipes que fazem análise forense, ou seja, que buscam evidências de algum crime realizado via Internet.

1.3.5 Autenticação

Esse serviço consiste em prover mecanismos para se identificar o usuário legítimo de um sistema ou aplicação. Os métodos de autenticação são muito difundidos e utilizados, e o mais comum é o uso de uma senha ou PIN. A autenticação também é um mecanismo que utilizamos para identificar a autenticidade de uma determinada mensagem.

Existem três mecanismos que podem ser utilizados na autenticação do usuário:

1) O que o usuário sabe: normalmente, é uma senha que o usuário ingressa no sistema. Deve-se buscar uma política de senha forte, uma vez que senhas muito óbvias podem ser adivinhadas, roubadas ou mesmo emprestadas. Embora não seja o melhor sistema de autenticação, é o mais utilizado.

2) O que o usuário possui: este método de autenticação é baseado no uso de cartões, tokens, chaves de encriptação ou certificados. O usuário deve apresentar algum desses dispositivos para ter acesso ao sistema. Hoje, a maior parte dos sistemas bancários no Brasil já utiliza os tokens. Os tokens geram OTPs (One Time Password), senhas válidas por apenas 30 segundos para acesso ao sistema.

3) O que o usuário é: este método de autenticação é baseado no uso da biometria. Cada pessoa possui características biométricas únicas, como impressão digital, íris ou geometria das mãos. Essas características biométricas podem ser utilizadas para autenticar os indivíduos.

1.3.6 Autorização

A autorização é o processo que ocorre posteriormente à autenticação. Depois que o usuário é autenticado, existe a necessidade de verificar os seus privilégios de acesso. A maioria das empresas, por questão de segurança, usa o princípio "need to know", ou seja, os usuários devem acessar o mínimo possível e necessário para que executem o seu trabalho.

Assim, um usuário com recursos básicos não deve, por exemplo, ter acesso de administração aos servidores. A autorização oferece uma série de recursos para que isso ocorra.

1.3.7 Auditoria

A auditoria tem uma importância fundamental. É a partir dela que criamos registros, os famosos logs, nos quais todas as ações e comportamentos realizados na rede e nas aplicações ficam registrados. Esses logs devem ser retidos e armazenados para análise.

A ideia da auditoria não é apenas encontrar usuários não autorizados que eventualmente estejam fazendo ações não permitidas, mas também monitorar os usuários autorizados para verificar se não estão realizando ações indevidas e mal-intencionadas quanto aos dados, rede e aplicações.

Lembra-se do exemplo que mencionamos do funcionário mal-intencionado que criou uma bomba-relógio? Ele só foi identificado devido a um processo de auditoria.

Os logs são fundamentais para identificarmos as tentativas de burlar a política de segurança, porém cada dispositivo e cada servidor podem gerar milhares de logs por dia. Isso significa que as empresas precisariam de equipes de auditoria muito grandes. Para resolver essa questão existem sistemas conhecidos como SIEM (Security Information and Event Management), que coletam os logs dos equipamentos e dispositivos (rede, servidores, storage, segurança), normalizam-nos (colocar em um formato padrão) e os armazenam em uma base de retenção de logs. Além disso, o SIEM permite fazer a análise em tempo real dos eventos que estão chegando, ajudando assim a identificar fraudes, acessos indevidos e ataques. Trata-se, portanto, de uma ferramenta fundamental na análise e gestão de segurança.

Os serviços de segurança têm uma importância fundamental, ainda que sua correta aplicação dependa da informação que desejamos proteger e do tipo de negócio. Por exemplo, para um banco, é muito importante garantir todos os serviços, mas em especial a confidencialidade dos dados do cliente. Por outro lado, para uma entidade sem fins lucrativos, esses serviços são importantes, porém não tão relevantes, em decorrência da natureza da informação que ela deseja proteger.

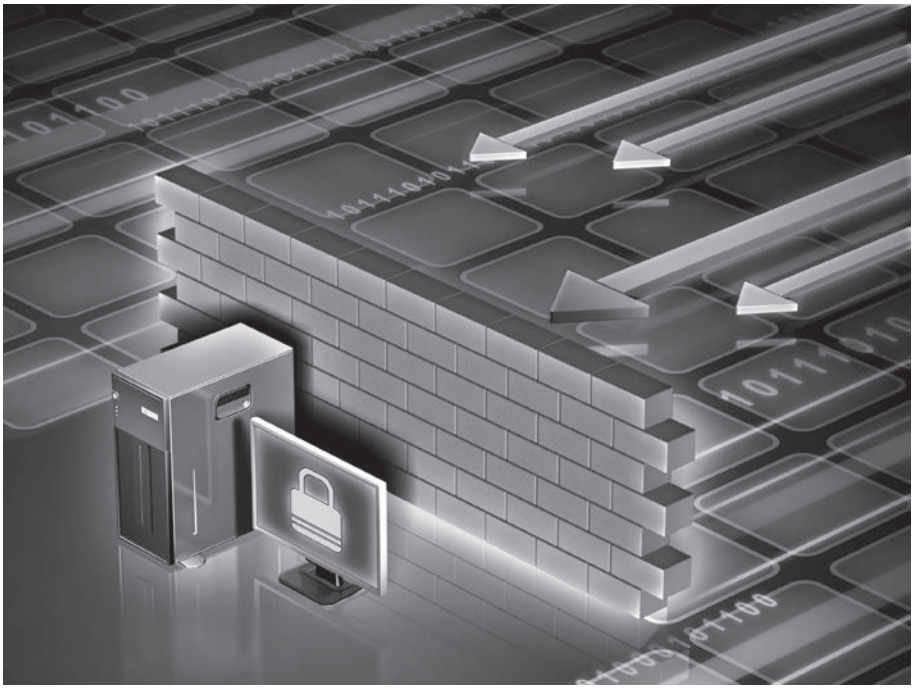
1.4 O papel do firewall

O firewall nos ajuda a proteger o perímetro da rede. Define-se por perímetro de rede a linha imaginária entre a rede interna da empresa, que devemos proteger, e a rede externa, que normalmente é desprotegida quando falamos de Internet.

Assim, o perímetro pode ser definido como todo ponto de acesso da rede externa à rede interna da empresa. Desde que começamos a migrar os sistemas de grandes computadores para sistemas em baixa plataforma, criando as redes locais da maneira que existem hoje, surgiu a necessidade de se estabelecer um perímetro de rede.

O firewall, ou "parede de fogo", tem um papel fundamental, porque é ele que vai separar a rede protegida – ou seja, a rede interna – da rede externa, que é desprotegida. Portanto, o firewall é a base da proteção perimetral.

O firewall é o elemento que irá realizar o controle de acesso, e isso ocorre por meio da implementação de ACLs (Access Control Lists), ou listas de controle de acesso. Essas listas são tabelas que definem, a partir da origem e do destino de cada pacote, se eles serão permitidos, monitorados ou bloqueados pelo firewall. Desse modo, o firewall acaba sendo um portão, ou seja, um controlador das conexões de rede que se originam e que passam por ele.



Andrea Danti/Shutterstock.com

Figura 1.3 – O firewall funciona como uma barreira que protege o computador de ataques externos.

1.4.1 Arquitetura de um ataque

Existe uma metodologia que os hackers utilizam para realizar ataques bem-sucedidos. Essa metodologia é composta de algumas etapas, e dentre elas podemos destacar: reconhecimento, scanning/varredura, enumeração, exploração de uma Vulnerabilidade e Preservação do Acesso.

1.4.2 Reconhecimento

Essa técnica consiste em buscar no Google, ou em informações de registros de domínios maiores, dados das empresas que o hacker deseja atacar. Localizar e verificar registros de DNS e com o WhoIS podem ajudar bastante na verificação de dados referentes a quem registrou um determinado domínio.

Em um ataque de reconhecimento conseguimos buscar informações também na própria página da empresa. Lá, muitas vezes encontramos nomes, endereços e e-mails de contato. Existem relatórios públicos de empresas que também fornecem uma boa ideia acerca de como elas estão estruturadas.

Existe um site chamado <http://www.archive.org> que permite ao usuário acessar versões de páginas que foram publicadas no passado. Esse também pode ser um importante mecanismo.

O Google hoje em dia é definitivamente uma das melhores ferramentas de ataque. Podemos usá-lo para fazer buscas customizadas visando coletar informações importantes, inclusive arquivos confidenciais que eventualmente estejam sendo indexados pelo próprio Google quando ele faz buscas no site da empresa.

1.4.3 Scanning/varredura

A partir do momento que sabemos o que queremos atacar e temos as informações detalhadas da empresa, como funcionários, e-mails e, principalmente, os endereços IP, vamos para a fase de scanning.

Essa fase consiste em utilizar um conjunto de ferramentas para identificar quais os sistemas operacionais e os servidores da empresa que estão publicados na Internet. Essa é a porta de entrada para um ataque bem-sucedido.

Na fase de scanning descobrimos também quais serviços estão sendo executados na máquina por meio da varredura de portas.

Tabela 1.1 – Principais serviços baseados nas RFC 1700 (“well-known ports”)

Porta	Protocolo	Serviço
21	TCP	FTP (serviço de transferência de arquivos)
25	TCP	SMTP (serviço de correio eletrônico)
53	TCP	DNS (serviço de nomes – converte domínios em endereços IP)
80	TCP	HTTP (protocolo web)
110	TCP	POP3 (envio de e-mails)
139	TCP	Netbios (protocolo Microsoft)
443	TCP	HTTPS (protocolo web seguro)

Após levantamento das portas e dos serviços descobertos, podemos passar para a próxima fase, que se chama enumeração. Uma das ferramentas mais utilizadas para a fase de scanning é o NMAP.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
Starting Nmap 6.47 ( http://nmap.org ) at 2015-02-14 03:01 EST
Nmap scan report for 192.168.0.150
Host is up (0.0011s latency).
Not shown: 990 closed ports
PORT      STATE SERVICE
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
443/tcp   open  https
445/tcp   open  microsoft-ds
548/tcp   open  afp
2049/tcp  open  nfs
3689/tcp  open  rendezvous
9000/tcp  open  cslistener
49152/tcp open  unknown
Device type: general purpose
Running: Linux 2.4.X|3.X
OS CPE: cpe:/o:linux:linux_kernel:2.4 cpe:/o:linux:linux_kernel:3
OS details: DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2

OS detection performed. Please report any incorrect results at http://nmap.org/s
ubmit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.09 seconds
root@kali:~#
```

Figura 1.4 – Execução do NMAP sobre um servidor.

No exemplo da Figura 1.4, observamos que o sistema operacional da máquina na qual realizamos a varredura é o Linux_Kernel 2.4.

1.4.4 Enumeração

A fase de enumeração tem como objetivo descobrir os banners do sistema, ou seja, quais as versões dos sistemas operacionais e das aplicações. A partir dessas informações, o hacker pode pesquisar e explorar as vulnerabilidades daquele servidor especificamente.

O hacker estabelece conexões com os servidores e os sistemas para ter acesso aos banners do sistema operacional. A partir desse banner ele tem uma ideia de qual versão está sendo utilizada. Esse tipo de informação é fundamental para se descobrir se aquela determinada versão está vulnerável a um determinado ataque e qual ferramenta deve ser utilizada.

Na Figura 1.5 podemos observar um banner de um serviço FTP. Por meio dele, conseguimos saber o serviço de FTP que está sendo executado no servidor – neste caso, o Pure – FTPd.

```
Administrator: C:\Windows\system32\cmd.exe - ftp 192.168.0.250
C:\Users\demoraea>ftp 192.168.0.250
Connected to 192.168.0.250.
220---------- Welcome to Pure-FTPd [TLS] ----------
220-You are user number 1 of 10 allowed.
220-Local time is now 05:29. Server port: 21.
220-This is a private system - No anonymous login
220-IPv6 connections are also welcome on this server.
220 You will be disconnected after 15 minutes of inactivity.
User (192.168.0.250:(none)): _
```

Figura 1.5 – Exemplo de verificação de banner.

1.4.5 Exploit – exploração da vulnerabilidade

Nessa fase, o hacker já pesquisou a vulnerabilidade que existe em determinada aplicação. Agora, resta apenas explorar essa vulnerabilidade para que ele obtenha acesso remoto à máquina.

Há uma série de ferramentas que permitem carregar e executar os temidos exploits, e a mais conhecida delas é o Metasploit.

Amplie seus conhecimentos

Você conhece o Kali Linux?

O Kali Linux é uma distribuição open source do Linux preparada com aplicativos cujo objetivo é permitir que o usuário realize testes de segurança em seu ambiente. O Kali é uma distribuição que evoluiu do Backtrack, também bem conhecida. Hoje, é uma das distribuições mais utilizadas por *pen testers*, ou seja, profissionais que realizam testes de invasão. Caso você queira explorar um pouco mais sobre esse leque de ferramentas, acesse <http://www.kali.org>.

O Metasploit permite carregarmos os payloads e executar a exploração da vulnerabilidade. Na figura a seguir podemos observar a GUI (interface) do Metasploit.

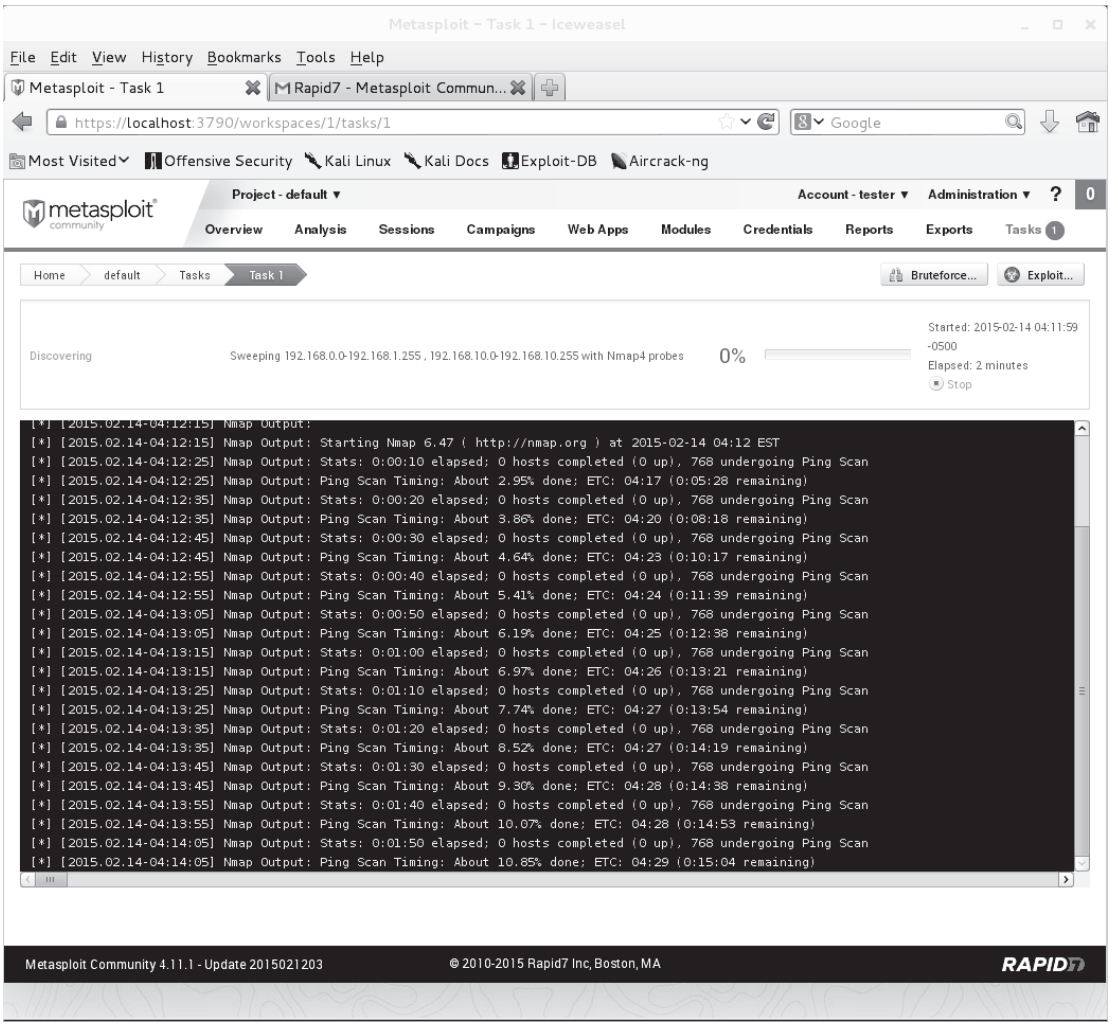


Figura 1.6 – O Metasploit.

1.4.6 Preservação do acesso

Para preservar o acesso, é interessante criarmos uma conta com direito de administrador para ser acessada *a posteriori* no sistema. Apagar os logs do sistema operacional para não deixar pegadas que evidenciem que a máquina foi atacada também é uma boa prática.

Vamos recapitular?

Neste capítulo aprendemos sobre conceitos de segurança da informação e os principais serviços de segurança (confidencialidade, integridade, disponibilidade, não repúdio, autenticação, autorização e auditoria). Vimos também qual a motivação para os principais tipos de ataque. Apresentamos uma introdução sobre o papel do firewall e do perímetro e concluímos com a motivação de um ataque.

Agora é com você!

1) O que é segurança da informação? Como podemos comparar o termo em inglês "safety" com o termo em português "segurança"?

2) No conceito de confidencialidade, qual processo desejamos proteger?

3) Qual a principal ferramenta utilizada para a garantir o processo de confidencialidade? O que devemos manter em segredo para garantir a confidencialidade?

4) A integridade é cada vez mais importante tanto no armazenamento como na transmissão das mensagens. Qual o dispositivo que utilizamos para verificar a integridade dos dados?

5) Sempre existe o risco inerente de um usuário negar uma ação que tenha realizado – como, por exemplo, o acesso indevido a dados e aplicações ou mesmo o envio de uma mensagem. Qual o serviço de segurança que devemos utilizar para tratar esse cenário?

6) O caso apresentado do bico do avião franco-britânico Concorde pode ser classificado em que tipo de motivação?

7) O que são os "script kids"? Qual o risco dessa ameaça?

8) Grupos como o Anonymous e o Lulzsec caracterizam qual tipo de ameaça?

9) Os firewalls são uma importante ferramenta de defesa. Explique qual o papel do firewall na defesa do perímetro.

2

Firewalls

Para começar

Este capítulo tem como objetivo apresentar os conceitos básicos da tecnologia de firewall, incluindo seu funcionamento, suas características, os tipos de firewall que existem e um exemplo prático de configuração.

A conexão com a Internet traz às corporações os seguintes riscos:

» Riscos relacionados aos dados (confidencialidade, integridade e disponibilidade).

» Riscos relacionados aos recursos e aos ativos da empresa.

» Riscos relacionados à imagem da empresa, uma vez que um ataque bem-sucedido pode representar um verdadeiro risco para a sua reputação caso seja divulgado.

Esses riscos ocorrem porque, normalmente, não existe uma política de segurança clara acerca das conexões com a Internet. Além disso, as redes que constituem a Internet também não são seguras e confiáveis. Um firewall é um equipamento de rede que desempenha um papel fundamental dentro desse cenário.

2.1 Firewall

O firewall, ou "parede de fogo", é um sistema que atua como ponto único de defesa entre a rede privada e a rede pública. Ele pode ainda controlar o tráfego entre as sub-redes de uma rede privada.

Basicamente, todo o tráfego de entrada e saída da rede deve passar obrigatoriamente por esse sistema de segurança. O firewall pode autorizar, negar e registrar tudo que passa por ele.

Embora existam muitos programas que se vendem com a denominação de firewall, um firewall não é um programa, e sim um conjunto de recursos de hardware e software destinados a garantir a segurança da rede. Suas principais funções:

- Estabelecimento de um perímetro de segurança.
- Separar as redes e controlar os acessos.
- Ser um elemento central de controle e aplicação de políticas de segurança.
- Proteger sistemas vulneráveis na rede.
- Aumentar a privacidade.
- Registrar e gerar estatísticas do uso da rede e acessos indevidos.

Um firewall pode ser tão simples quanto um roteador que aplica um filtro de pacotes ou tão complexo quanto um gateway que combina funções de filtros de pacotes e proxy na camada de aplicação. O firewall é sempre proprietário, pois a regra é não seguir padrões para aumentar a segurança.

O firewall controla todas as mensagens que passam por ele. Em geral, um firewall é utilizado para interconectar uma rede segura (como a rede interna das empresas) a uma rede insegura, como a Internet.

Em sua configuração padrão, os firewalls barram todos os tráfegos que passam por ele. Assim, o administrador de segurança, a partir da definição de uma política de segurança, deve configurar regras no firewall para que sejam liberados os tráfegos permitidos. Um exemplo é o servidor de e-mail. Caso não se crie uma regra no firewall liberando a porta 25 para o servidor de e-mail, a empresa não poderá receber nenhuma correspondência eletrônica, pois o firewall bloqueará esses pacotes. As empresas usam os firewalls também para restringir o tráfego de saída, ou seja, dos usuários internos à Internet. Isso se faz, geralmente, mediante o uso de filtros de conteúdo, cujo objetivo é restringir o acesso a páginas não autorizadas (por exemplo, páginas de conteúdo indevido, como sites de jogos, músicas ou mesmo de pornografia).

Um firewall pode ainda ser utilizado na proteção entre redes internas da mesma empresa. Por exemplo, um banco pode querer isolar a rede da tesouraria do resto da rede, permitindo, com a adoção do firewall, um nível de segurança ainda maior para esses usuários. Afinal, essa providência impede que exista um ataque proveniente da rede do banco à rede da tesouraria.

Os firewalls, além de controlar os acessos, possuem recursos para registro detalhado dos usuários e do tráfego que passa por ele.

Essa solução nos permite estabelecer o que conhecemos como perímetro de segurança, além de separar e segregar a rede interna controlando os acessos e aplicar a política de segurança. Um firewall pode ser tão simples quanto um roteador que filtra pacotes com base em um ACL (Access Control List) ou lista de controle de acessos, mas pode ser tão complexo quanto um firewall de aplicação, que filtra e analisa os pacotes até a camada de aplicação antes de tomar a decisão de liberar o bloquear o pacote.

Normalmente, as políticas de um firewall podem ser aplicadas diferentemente para o tráfego entrante e o de saída. Como em outras soluções de segurança, não existe padronização para esse tipo de solução.

As ações que podem ser tomadas por um firewall são: autorizar, negar ou simplesmente registrar os acessos realizados.

2.2 Roteador de perímetro

O roteador de perímetro desempenha um papel fundamental de segurança. Ele é o primeiro dispositivo no qual se pode criar o primeiro controle de acesso. Como o roteador desempenha o papel de filtro com as suas listas de acesso ou ACLs, muitas vezes classificamos a atuação do roteador de perímetro como uma primeira camada de firewall.

As listas de acesso de um roteador são mais simples e, normalmente, classificam-se como filtros de pacotes simples. Os roteadores, por serem equipamentos de camada 3, possuem pouca ou nenhuma interferência quanto aos protocolos de aplicação. Normalmente, em sua lista de acesso, um roteador toma a decisão de permitir ou negar determinado tipo de tráfego com base nas seguintes informações:

- Endereço de origem.
- Endereço de destino.
- Porta de origem.
- Porta de destino.

2.3 Bastion host

Um bastion host é uma máquina ou sistema (por exemplo, servidores web, FTP ou os próprios roteadores) que pode estar exposto a um hacker e necessita de proteção.

Muitas pessoas confundem o termo bastion host com o termo firewall. Um bastion host é simplesmente um sistema que precisa ser protegido contra um ataque. Todos os firewalls podem ser considerados bastion hosts, uma vez que não devem ser alvos de ataques. Normalmente, os servidores e serviços da empresa precisam ser devidamente atualizados, do mesmo modo que os serviços desnecessários devem ser desabilitados nesses computadores. O processo de deixar o sistema operacional mais protegido, desabilitando serviços vulneráveis, é conhecido como "hardening" do sistema operacional.

Normalmente, os bastion hosts são os sistemas críticos que devem ser protegidos por um firewall, pois é usual que esses sistemas estejam publicados e expostos na Internet.

2.4 DMZ

No jargão militar, por definição, uma DMZ (ou Zona Desmilitarizada) é uma fronteira entre duas potências militares na qual não se permite o uso de armamentos.

Na área de segurança de redes, uma DMZ é uma rede física ou uma sub-rede que contém servidores e serviços que estarão disponibilizados para acessos provenientes de uma rede não confiável, como a Internet. Normalmente, é na DMZ que colocamos os servidores públicos de web, FTP e de correio eletrônico das empresas. O propósito da DMZ é garantir uma proteção adicional à rede local

(corporativa) isolando o tráfego proveniente da Internet para os servidores públicos da empresa da rede corporativa. Ou seja, evita-se que esse tráfego, que pode ser malicioso (uma vez que é proveniente de redes não confiáveis, como a Internet), passe por dentro da rede corporativa.

2.5 Rede externa WAN

Em geral, os firewalls são alocados para o acesso à Internet, portanto, podemos considerar essa rede como sendo a Internet. É bom lembrar que todos os endereços dessa rede são válidos, portanto, a interface externa do firewall deve possuir um endereço válido na rede.

2.6 Rede interna LAN

Corresponde à rede interna da empresa que desejamos proteger. Em geral, as máquinas dessa rede trabalham com endereços não registrados ou inválidos, cabendo ao firewall a função de NAT já descrita anteriormente. O tráfego interno dessa rede, ou seja, o que não trafega para a Internet, não consegue ser tratado pelo firewall em virtude de não passar por ele.

Na Figura 2.1 podemos observar a estrutura de conexão da rede com um firewall de três interfaces:

» DMZ: onde se encontra publicado o servidor com as páginas públicas da empresa.

» LAN: interface para a rede corporativa.

» WAN: interface conectada diretamente ao roteador da Internet.

A linha pontilhada separa o que conhecemos de Zona Militarizada da Zona Desmilitarizada. A Zona Desmilitarizada é a zona não protegida pelo firewall, enquanto a Zona Militarizada é a zona que possui proteção pelo firewall.

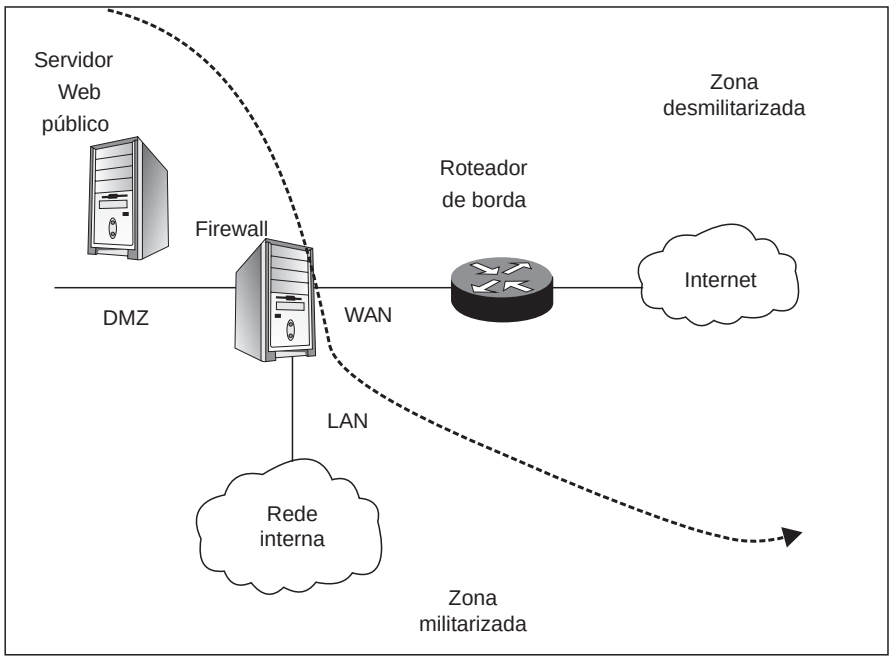


Figura 2.1 – Arquitetura do firewall na rede.

As primeiras arquiteturas de firewall isolavam as redes em nível lógico. Hoje existem firewalls dos seguintes tipos:

» Filtros de Pacotes: checa todos os pacotes e verifica, de acordo com uma lista chamada ACL ("Access List"), se o pacote checado será bloqueado ou permitido.

» Stateful Inspection: examina a aplicação e a identificação do pacote conforme um contexto.

» Circuit Level Gateways ou Gateways de Aplicação: examina o pacote em detalhes, verificando inclusive o seu conteúdo.

2.7 Filtros de pacotes

Os filtros de pacotes atuam verificando apenas os endereços IP e as portas TCP/UDP. Esses firewalls trabalham com uma lista de controle de acesso, também conhecida como "Access List", que é verificada antes que um pacote seja encaminhado para a rede interna. A lista relaciona o tráfego que é permitido e o que deve ser bloqueado.

Vantagens:

» Rapidez e eficiência.

» Facilidade de compreensão.

» Transparência.

» Disponibilidade em diversos dispositivos.

» Flexibilidade.

Desvantagens:

» O tráfego entre as redes não é totalmente isolado.

» Requer muitos testes para verificação das funcionalidades.

» Em geral, a aplicação de políticas é difícil.

» Sintaxe difícil: os processos de controle e administração das listas de acesso são complexos e trabalhosos.

» O processamento dos pacotes nos filtros se restringe à camada de transporte do modelo OSI.

» A inspeção é feita em um pacote por vez.

» Está sujeito a ataques de fragmentação.

» Os recursos de logs e auditoria são mínimos.

» Não esconde automaticamente os endereços de rede.

» Não avalia o tamanho do cabeçalho IP.

O filtro de pacotes não faz nenhuma alteração no pacote que passa pelo firewall.

A primeira ou última regra da lista de acesso deve negar todo o tráfego não explicitamente permitido. Como consequência, cada lista necessita de pelo menos uma permissão para permitir o tráfego. Na Tabela 2.1 observamos uma lista de acesso.

Tabela 2.1 – Lista de acesso

IP da Origem	Porta na Origem	IP do Destino	Porta no Destino	Ação	Registro

Os critérios de avaliação, de acordo com os quais o pacote passará ou será bloqueado, são:

» Lista de controle de acesso.

» Avaliação do ID do protocolo.

» IP de origem.

» Porta de origem.

» IP de destino.

» Porta de destino.

A Figura 2.2 apresenta o funcionamento em nível de camada OSI do filtro de pacotes.

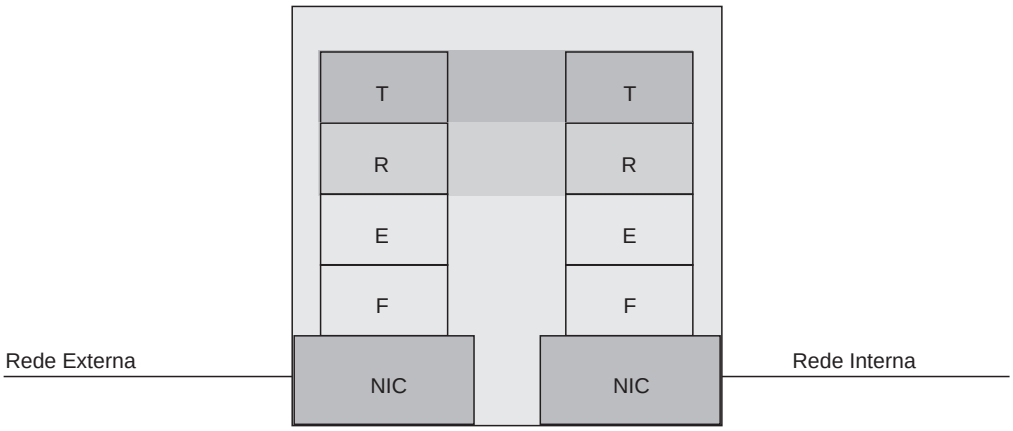


Figura 2.2 – Funcionamento em nível de camada OSI do Filtro de Pacotes.

2.8 Stateful inspection – "verificação por contexto"

Nessa arquitetura, cada pacote é individualmente verificado de acordo com o pacote anterior ou subsequente. Existe, portanto, uma verificação de contexto. Os pacotes são verificados mediante um fluxo de comunicação.

O Stateful Inspection examina os pacotes com base no estado da sessão da aplicação TCP ACK#, SEQ#, informações de portas etc. Os pacotes são examinados usando-se informações de dados de comunicações passadas. Esses firewalls têm ainda a habilidade de criar sessões de informação virtual para manter a inspeção sobre protocolos não orientados à conexão de pacotes que possam ter conteúdo não legal.

Os principais critérios de avaliação são:

» Lista de acesso (ACL).

» Regras de autorização.

» Verificação de padrões conhecidos de bits ou bytes.
» Avaliação do cabeçalho.
» Verificação do endereço IP de origem.
» Tamanho do cabeçalho IP.
» Indicador do fragmento IP.
» Avaliação do status da conexão.

2.8.1 Características adicionais

Além desses critérios, esse tipo de firewall deve ser capaz de prover serviços de roteamento. A verificação do contexto pode exigir muito da CPU em um proxy de aplicação, não gerando muitas vezes o benefício esperado.

Um firewall stateful apenas enviará respostas de DNS se elas estiverem associadas a uma query interna de DNS, ou seja, ele não aceita uma resposta caso não tenha enviado uma requisição. No caso do Telnet, uma sessão em andamento deve ser avaliada com base no fluxo apropriado da sequência de números e ACKs.

A Figura 2.3 mostra as camadas usadas para as decisões de filtragem.

O processamento de pacotes por um filtro stateful envolve a verificação nas camadas de transporte e sessão, fazendo a associação da quíntupla: Endereço IP Remoto + Endereço IP Local + Porta Remota + Porta Local + Protocolo de Transporte.

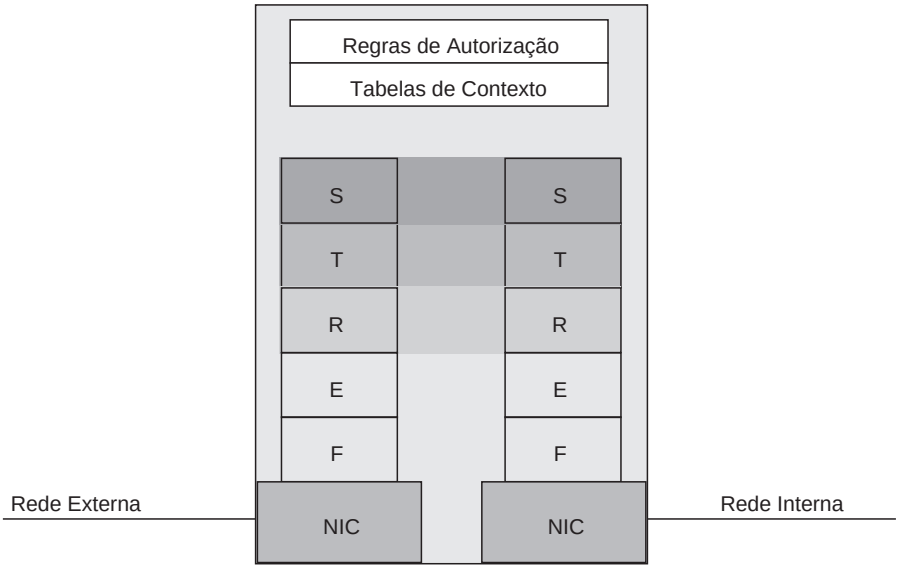


Figura 2.3 – Camadas OSI utilizadas na verificação do contexto.

2.9 Proxy

O proxy é um servidor que literalmente faz a intermediação da comunicação entre um equipamento na rede segura e um equipamento na rede externa. Vamos imaginar que um computador

A deseja se comunicar com um computador B: todas as conexões entre eles devem ser estabelecidas pelo proxy. Assim sendo, o computador A realiza uma conexão com o proxy, e o proxy estabelece uma conexão com o computador externo à rede (B), tornando-se então o responsável pela monitoração e pelo controle do tráfego trocado.

Vantagens:

» As redes são totalmente isoladas umas das outras.

» Recursos de log/Registro.

» Recursos de cache.

» Balanceamento de carga.

Desvantagens:

» São mais lentos e menos flexíveis;

» Podem exigir configuração dos clientes;

» Existe a necessidade de os proxies passarem por update para cada novo serviço ou aplicação criados e inseridos na rede.

Fique de olho!

Proxy é um termo em língua inglesa que significa procurador, ou seja, o proxy é como alguém que foi autorizado a fazer algo por você, gerenciando e coordenando as sessões de rede.

Os dados são analisados e modificados em nível de protocolo de aplicação, ou seja, o pacote é todo reescrito e remontado pelo proxy.

Os proxies podem ser transparentes e, nesse caso, não existe nenhum tipo de configuração das máquinas clientes ou não transparentes, o que já exige configuração.

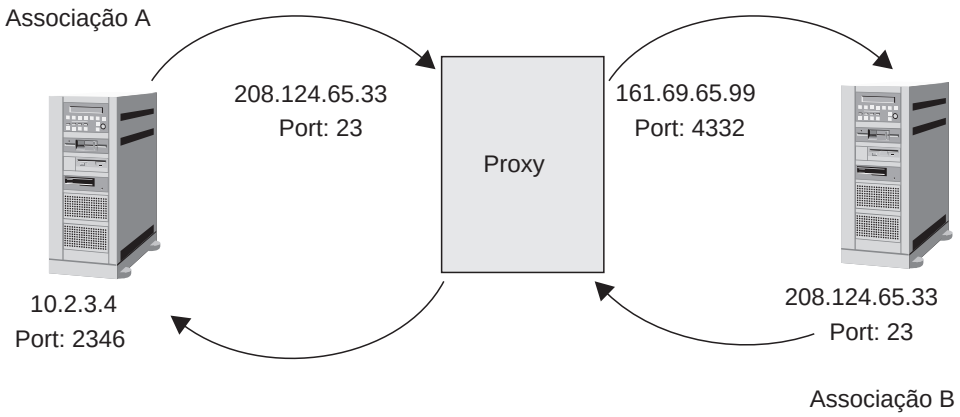


Figura 2.4 – Funcionamento do proxy.

Na Figura 2.4 a máquina interna inicia uma conexão, usando para isso o endereço IP remoto, a porta remota e o protocolo de transporte. O proxy fica posicionado no meio, interceptando a requisição, avaliando e iniciando a conexão com a máquina externa (destino). O proxy usa o endereço

IP externo próprio como origem, e cria seu próprio número de sequência. A resposta da máquina remota é enviada de volta para o proxy, que, por sua vez, casa a resposta com a requisição inicial da máquina interna, que então remonta o pacote enviado com o endereço da máquina interna como destino e com o endereço de origem da máquina remota e da porta remota.

Se o recurso de transparência não é usado, a máquina interna deve estar configurada para trabalhar com o proxy. Em vez de os pacotes serem direcionados para a máquina remota, eles inicialmente são enviados ao proxy, que efetiva a comunicação e envia a resposta à máquina de origem.

Existem proxies que trabalham apenas em nível de circuito, criando associações completas entre o cliente e o servidor sem a necessidade de interpretação do protocolo de aplicação.

Os pacotes são tratados pelo proxy segundo um critério de avaliação que inclui regras de autorização, tabelas de associação e avaliação do cabeçalho.

Quando utilizamos um proxy, as conexões podem apenas ser executadas pelo proxy, que tem a função de separar a rede interna da externa.

2.9.1 Proxy na camada de aplicação

Além dos atributos do proxy em nível de circuito, esse tipo de proxy executa o processamento de protocolos na camada de aplicação. Os critérios de avaliação usados para o pacote ser permitido ou negado são:

- Autenticação do usuário.
- Tabelas de associação.
- Regras de autorização.
- Regras de aplicação.
- Avaliação do cabeçalho.
- Auditoria.

Os proxies de aplicação trabalham com dados complexos das camadas de aplicação, detectando tentativas de quebra de segurança. Justamente devido a essas funcionalidades, são mais lentos que firewalls baseados em filtro de pacotes. Devido à interatividade com as aplicações, esses proxies não estão disponíveis para alguns tipos de serviço de aplicações específicas. A Figura 2.5 apresenta as camadas OSI utilizadas na decisão por um proxy.

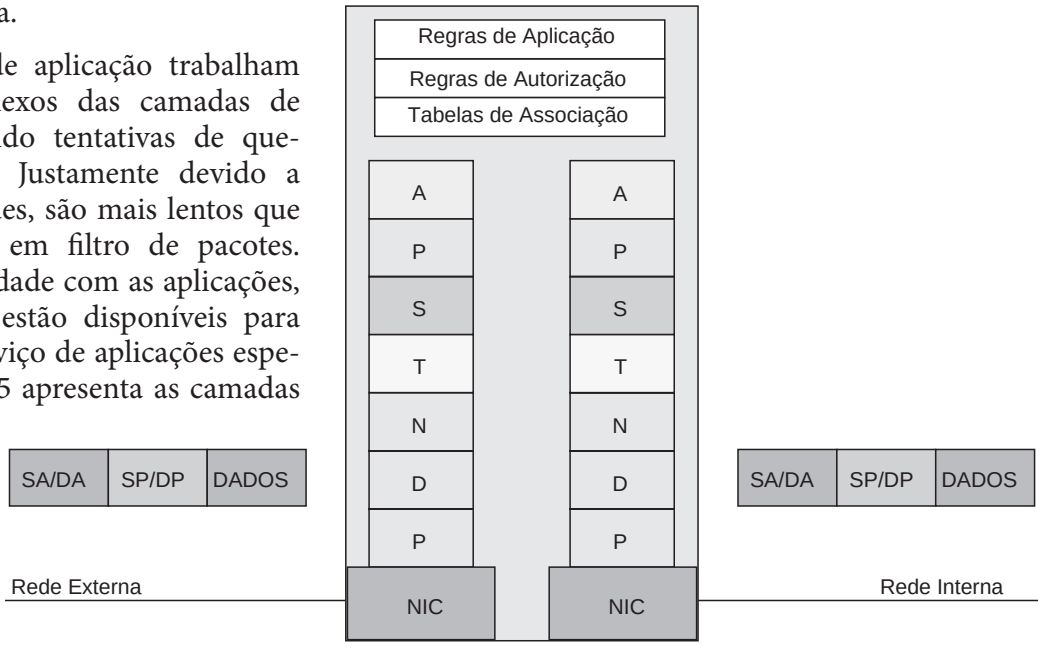


Figura 2.5 – Camadas OSI utilizadas no proxy.

2.9.2 Passos da política de segurança em um firewall baseado em proxy

Os principais passos para configurar uma política de segurança em um firewall:

» Determinar os tipos de proxy usados no firewall.

» Listar as máquinas internas que poderão usar o proxy.

» Ajustar os requerimentos de permissão ou negação a determinados destinos e os requisitos de autenticação.

O padrão é definir as seguintes permissões:

» Da rede interna, permitir FTP, TELNET, NNTP, NetShow, Real Audio, HTTP.

» Da rede externa, permitir POP3 e, eventualmente, FTP e TELNET.

» O endereço de origem ou o nome do host deve ser usado para determinar a política aplicável.

» Algumas regras podem ser aplicadas a grupos de máquinas, criando-se políticas de segurança gerais.

2.9.3 Principais tipos de proxies

» Proxies de aplicação: WWW, FTP, TELNET, MAIL, NNTP, SQL etc.

» Proxies em nível de circuito: que estejam em nível de rede (endereços IP e portas TCP/UDP).

» Proxies reversos: trabalham na forma reversa, permitindo o acesso a recursos internos.

» Proxies de cache: retêm os sites mais usados para reúso, sem a necessidade do acesso direto à Internet.

Tabela 2.2 – Comparativo entre os tipos de firewalls

	Autenticação	Autorização	Auditoria
Filtro de Pacotes Simples	Não	Sim, apenas endereços IP	Não
Filtro de Pacotes Stateful	Não	Sim	Limitado
Proxy a nível de circuito	Não	Sim	Limitado
Proxy a nível de aplicação	Sim	Sim, endereços IP e ID de usuários	Sim

2.10 Firewall proxy e filtro

Essa arquitetura de firewall trabalha tanto no modo proxy como no modo filtro. O modo filtro é usado para bloquear e filtrar o tráfego de serviços considerados seguros, enquanto o modo proxy é aplicado sobre um serviço inseguro que necessite do nível de segurança de um proxy. Na Figura 2.6 podemos observar um firewall baseado em proxy. É importante notar que as estações da rede devem possuir a configuração do browser para apontar para o proxy. Nesse caso, devem estar configurados o endereço da interface de rede local do proxy, 192.168.1.254, e a porta em que o serviço de proxy vai estar ativo – no caso, 3128. Veja a configuração na Figura 2.7.

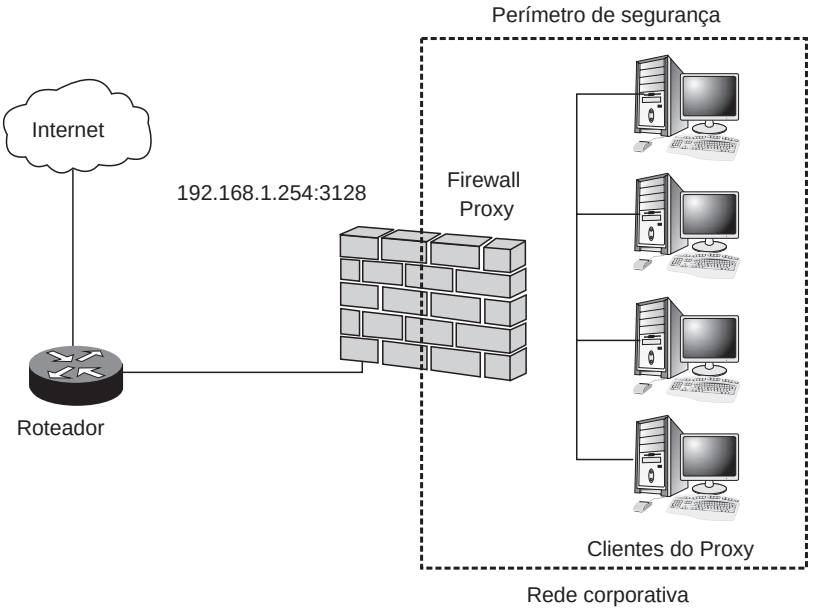


Figura 2.6 – Arquitetura de firewall proxy.

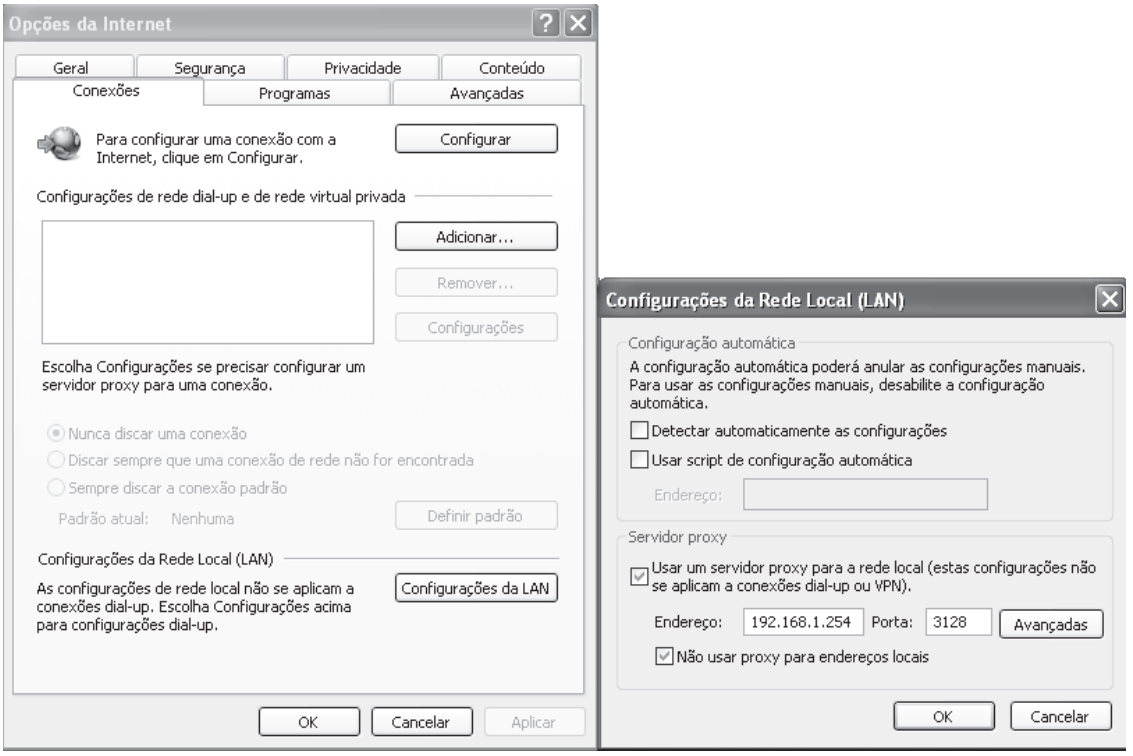


Figura 2.7 – Configuração de proxy no Internet Explorer.

Para configurar as opções de proxy no Microsoft Internet Explorer, vá a “Opções da Internet”, escolha “Configurações da Rede Local”, adicione no “Servidor Proxy” o endereço IP e a porta a ser utilizada pelo serviço de proxy.

Além de monitorar o tráfego entre redes, um firewall pode também desempenhar as seguintes funções:

1) Análise de conteúdo (Content Screening).
2) Gateway de VPN (Virtual Private Network).
3) Tradução de endereços de rede NAT (Network Address Translation).
4) Autenticação de usuários.
5) Balanceamento de carga (Load Balancing).

2.10.1 Análise de conteúdo

Um firewall pode ser usado para bloquear determinadas URLs, como de sites pornográficos, de piadas, de jogos e, enfim, páginas cujo conteúdo não faça parte da política de segurança da empresa. Essas listas de sites proibidos podem ser inseridas manualmente no firewall a partir de regras ou dinamicamente, utilizando-se um software que se agrega à solução de firewall e recebe diariamente a lista de distribuição de sites não permitidos.

2.10.2 Gateway de VPN

Um firewall pode, além de executar as funções de controle de acesso e do tráfego, funcionar como um gateway de VPN (Virtual Private Network), realizando conexões criptografadas e tuneladas, usando para isso um protocolo como o IPSEC, que implementa algoritmos criptográficos como o AES e o 3DES.

2.10.3 NAT

O NAT foi uma solução introduzida pela Cisco Systems que resolve a maior parte dos problemas relacionados ao esgotamento do número de endereços IP da Internet. O firewall que executa NAT realiza um mapeamento entre endereços da Internet válidos e inválidos (que são utilizados pelos computadores da rede interna), tornando-se desnecessário que cada estação possua seu próprio endereço IP válido na Internet.

O mapeamento entre os endereços válidos e inválidos pode ocorrer das seguintes formas:

» Único, ou seja, existe um único endereço inválido mapeado em um endereço válido.
» Um para um, o que significa que para cada endereço inválido deve existir um endereço válido.
» Muitos para um, a forma mais utilizada, em que muitos endereços inválidos compartilham o mesmo endereço válido.

O mapeamento do NAT pode ser visto na Figura 2.8.

O uso do NAT aumenta ainda mais a segurança da rede interna, porque os endereços das estações ficam mascarados.

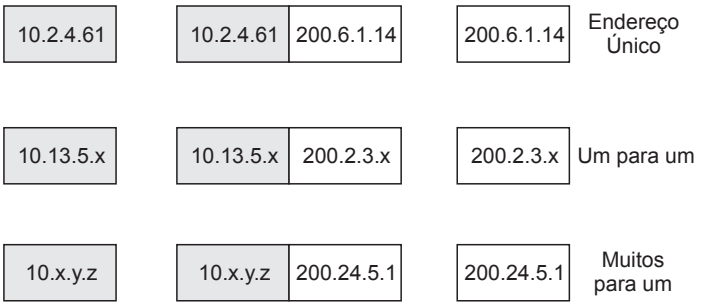


Figura 2.8 – Mapeamento dos endereços com NAT.

2.10.3.1 Autenticação de usuários

Os usuários externos à rede podem ser autenticados no firewall para ter acesso a algum servidor ou aplicação. Esse processo, em geral, leva em conta o uso de um servidor de autenticação RADIUS.

Essa autenticação pode ser configurada para ser solicitada quando do acesso da página html. Nesse caso, abre-se um menu pop-up para o usuário ser autenticado, entrando com seu login e senha.

2.10.3.2 Balanceamento de carga

O firewall pode executar o balanceamento de carga entre servidores, gerenciando assim a carga entre eles com base no tempo de resposta de cada servidor.

2.10.3.3 Limitações de um firewall

O firewall só controla o tráfego que passa por ele. Assim sendo, não oferece qualquer proteção contra ataques provenientes de usuários internos à rede cujo tráfego não passe por ele.

A Figura 2.9 apresenta um usuário burlando a proteção do firewall. Ele está fazendo um acesso direto à internet via modem 3G conectado à sua máquina.

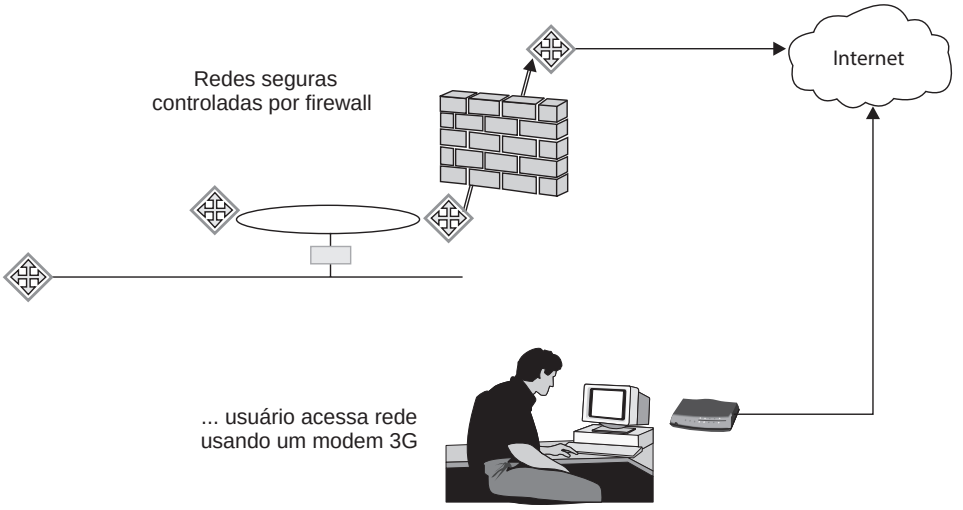


Figura 2.9 – Usuário burlando o firewall via acesso direto com um modem 3G.

Existem alguns ataques que os firewalls não conseguem evitar, como:

» Ataques ("exploits") contra vulnerabilidades em portas padrão, por exemplo, a porta 80, que fica aberta.

» Alguns tipos de "Denial of Service".

» Autenticação fraudulenta.

» Backdoors.

» Erros humanos.

Amplie seus conhecimentos

Como é possível bloquear um ataque sobre uma porta aberta de um firewall? Na verdade, o firewall com recursos tradicionais não tem essa capacidade, por isso, faz-se necessária a utilização de uma tecnologia que realize uma inspeção profunda nos pacotes – ou seja, que analise até a camada de aplicação. Essa tecnologia é conhecida como IPS (Intrusion Prevention System, ou sistema de prevenção a invasões). Os firewalls tradicionais podem vir com um módulo incorporado que execute a função de IPS, porém, normalmente, trata-se de um equipamento à parte, que trabalha em modo bridge (ou seja, sem configuração de endereço IP) e inspeciona o tráfego em linha. Esses equipamentos têm a capacidade de detectar e bloquear ataques em tempo real.

2.11 IP Tables

O IP Tables é uma aplicação em Linux que permite a configuração das regras de acesso do firewall do Kernel do Linux, o Netfilter. O Netfilter permite que os módulos do Kernel do Linux controlem diretamente os registradores e as funções da pilha de rede. O IP Tables é um firewall que realiza stateful inspection, ou seja, ele analisa os status das conexões.

O IP Tables permite criar um conjunto de regras, e cada regra possui um classificador e uma determinada ação.

Capacidades do IP Tables:

» Criação de um firewall filtro de pacotes stateful tanto com IP versão 4 como com IP versão 6.

» Criação de regras de NAT (Network Address Translation).

» Suporte a SNAT – NAT estático.

» Integração com a camada de aplicação com APIs de terceiros.

» Grande número de plug-ins.

» Rejeita automaticamente pacotes malformados.

» Realiza roteamento dos pacotes.

» Permite priorizar alguns tipos de serviços.

» Redirecionamento de portas.

» Detectar pacotes fragmentados.

» Contabilização dos pacotes nas interfaces.

A Figura 2.10 apresenta como o IP Tables faz o tratamento dos pacotes, desde a sua entrada até a saída pelo firewall.

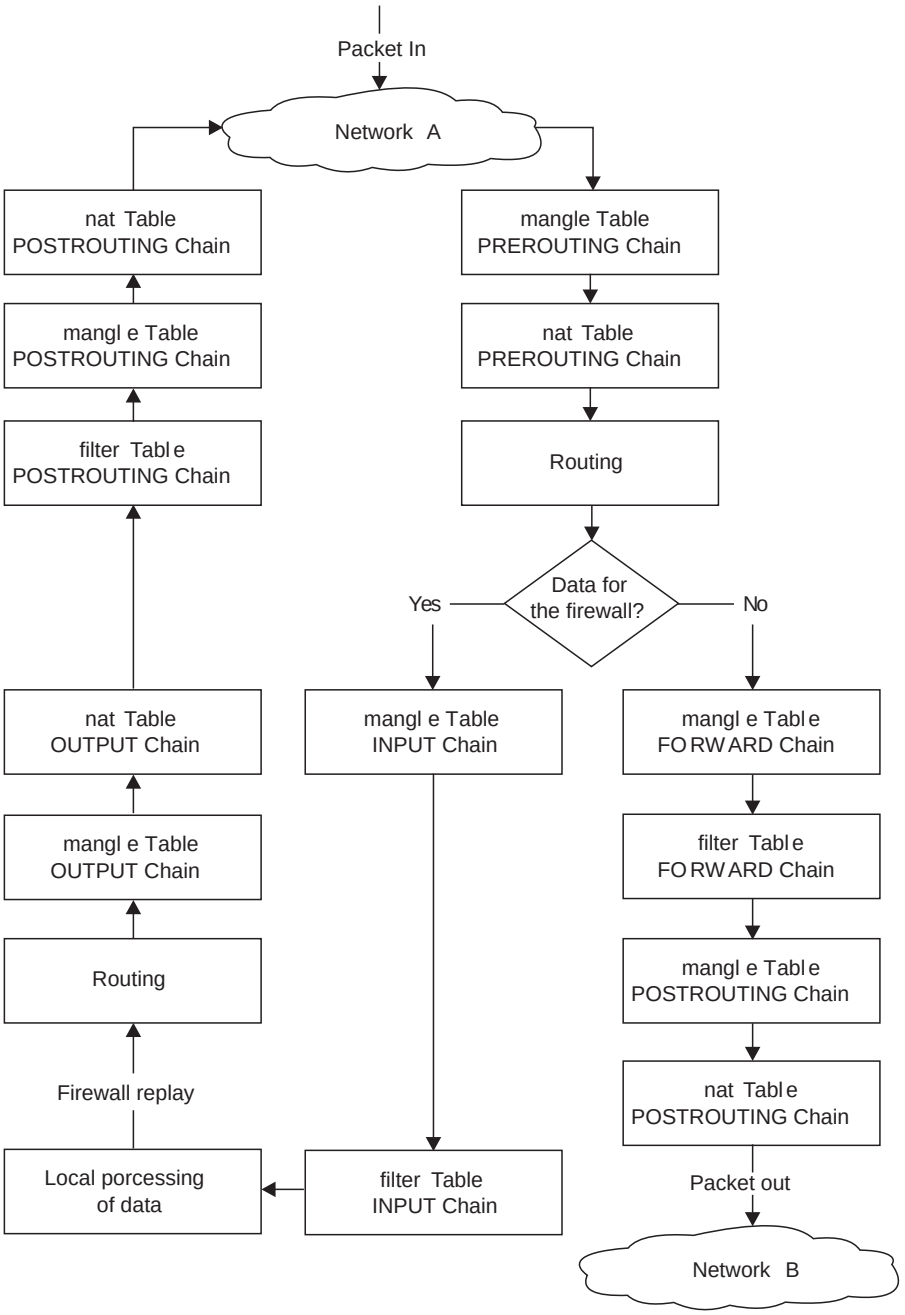


Figura 2.10 – Tratamento dos pacotes pelo IP Tables.

2.12 Política de segurança em um firewall

A política de segurança em um firewall busca definir que ação deve ser tomada por ele em determinada situação. Perguntas que normalmente são levantadas quando definimos a política de segurança em um firewall incluem:

» Quais processos de proxy deverão estar ativados e quais requerem autenticação?

» As políticas foram definidas para acessos provenientes da rede interna à Internet e vice-versa?

» Foram definidos quais os tipos de acesso permitidos à DMZ?

A filosofia de projeto de segurança deve seguir o que conhecemos como política restritiva, ou seja, todos os serviços disponíveis pela rede devem ser negados, e o usuário autoriza apenas os tráfegos e serviços que devem ser permitidos. Embora a estratégia de negar tudo seja radical, ao longo dos anos ela demonstrou ser a mais eficiente, principalmente porque novas ameaças surgem a cada dia e não conseguimos prever qual serviço e qual porta elas vão utilizar para se propagar.

Isso significa dizer que, se o ambiente está todo fechado, provavelmente a ameaça é alguma porta da aplicação estar aberta ou não no firewall. Se não for um serviço de uso comum na rede, com certeza a porta estará fechada, garantindo-se assim a segurança.

Se existir algum serviço que necessite de autenticação no firewall, não permita que as contas configuradas para o serviço tenham direitos de administrador no firewall, pois, se alguém conseguir comprometer uma senha que tenha direito de administração, o estrago vai ser muito grande.

Habilite sempre o log no firewall para controlar alterações de política e configuração. Além disso, é uma boa prática sempre inspecionar em tempo real o tráfego que está passando pelo firewall.

Crie sempre a área protegida isolando o perímetro da rede das redes inspecionadas e protegidas pelo firewall.

Defina os mecanismos de segurança no perímetro, e é muito positivo que implementemos regras de bloqueio de alguns protocolos indesejáveis já no roteador de borda.

Toda a comunicação que saia ou entre na rede corporativa deve ser monitorada por um firewall. Não devemos permitir acessos diretos e sem controle pelo firewall, como observamos na Figura 2.10.

Na hora de configurar as políticas no firewall, as mais específicas sempre vêm na frente das mais genéricas.

Crie uma rede em separado, como uma VLAN, para o gerenciamento do firewall, evitando dessa maneira um ataque ao console do firewall, cujo objetivo seria o de causar indisponibilidade ou mesmo reconfigurações não autorizadas.

Configure de maneira adequada as regras de NAT, incluindo aí o NAT estático, para serviços que precisem de um mapeamento direto com um endereço público, como é o caso de um servidor publicado na Internet.

Configure adequadamente os serviços que vão ser bloqueados no nível de rede com base no IP e no Protocolo e os serviços que vão ser bloqueados no nível de aplicação via configuração de proxy como o HTTP.

2.13 Caso prático

A empresa ACME possui um provedor de serviço que registrou o seu domínio como <http:// www.acme.com.br>.

O firewall deve estabelecer um perímetro de segurança para proteger a rede interna de acessos externos indevidos.

De acordo com a política de segurança da empresa sobre aplicações, o firewall deve determinar se aceita ou não o tráfego dessas aplicações.

O firewall deve implementar uma DMZ na qual estarão publicados os seguintes serviços:

» Servidor Web no endereço de DMZ 172.16.10.10/16

» Servidor SMTP no endereço de DMZ 172.16.10.20/16

» Servidor de DNS na DMZ 172.16.10.30/16

» Servidor FTP na DMZ 172.16.10.40/16

Na Figura 2.11 observamos o desenho da arquitetura.

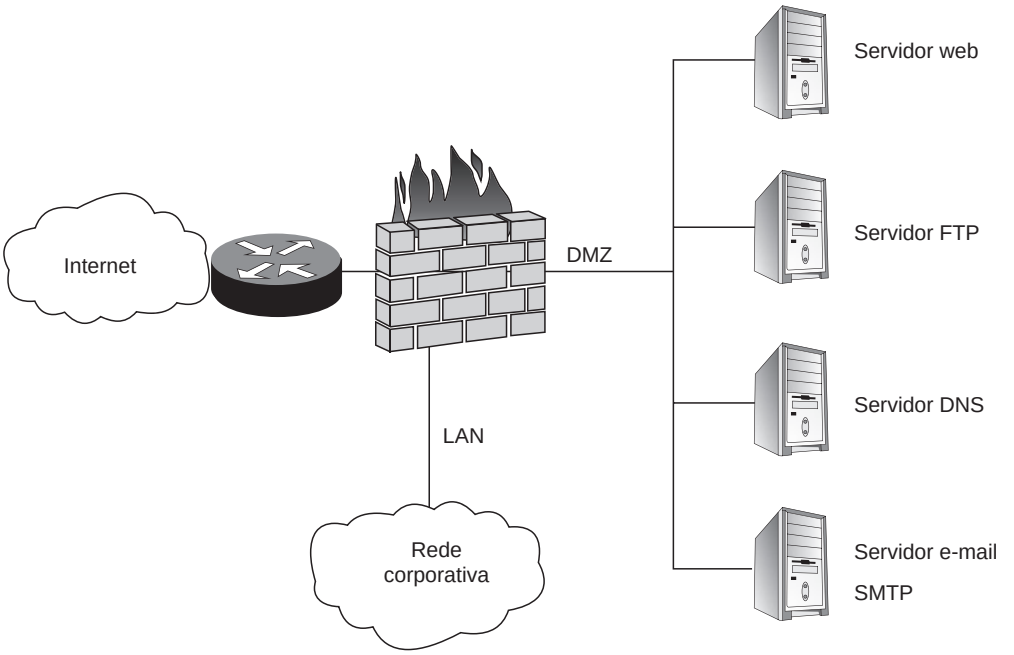


Figura 2.11 – Arquitetura.

A Tabela 2.3 apresenta as políticas de configuração para atender a essa demanda. Observe que o acesso à Internet dos usuários da LAN está bem restritivo. Eles praticamente só conseguem acessar a web, HTTPS e FTP externamente.

Tabela 2.3 – Políticas de acesso

Serviço	Porta	Origem	Destino	Ação
Web	80	Internet	DMZ	Permite
Web	80	Lan	DMZ	Permite
Web	80	DMZ	Internet	Permite
Web	80	Lan	Internet	Permite
Web	80	Internet	Lan	Nega

Serviço	Porta	Origem	Destino	Ação
FTP	21	Internet	DMZ	Permite
FTP	21	Lan	DMZ	Permite
FTP	21	DMZ	Internet	Permite
FTP	21	Lan	Internet	Permite
FTP	21	Internet	Lan	Nega
FTP_data	20	Internet	DMZ	Permite
FTP_data	20	Lan	DMZ	Permite
FTP_data	20	DMZ	Internet	Permite
FTP_data	20	Lan	Internet	Permite
FTP_data	20	Internet	Lan	Nega
DNS	53	Internet	DMZ	Permite
DNS	53	Lan	DMZ	Permite
DNS	53	DMZ	Internet	Permite
DNS	53	Lan	Internet	Nega
DNS	53	Internet	Lan	Nega
SMTP	25	Internet	DMZ	Permite
SMTP	25	Lan	DMZ	Permite
SMTP	25	DMZ	Internet	Permite
SMTP	25	Lan	Internet	Nega
SMTP	25	Internet	Lan	Nega
HTTPS	445	Lan	Internet	Permite
HTTPS	445	Internet	Lan	Nega
HTTPS	445	Internet	DMZ	Nega

A seguir, apresentamos uma configuração genérica do IP Tables que permite que apenas os serviços identificados sejam acessados da Internet para a DMZ, bloqueando-se todos os outros serviços.

2.13.1 Configuração IP Tables

```
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:LINWIZ-INPUT - [0:0]
:REJECT-PKT - [0:0]

-A INPUT -j LINWIZ-INPUT

#######################################################################
# Permite Tráfego de Loopback
```

```
-A LINWIZ-INPUT -i lo -j ACCEPT

# Bloqueia tentativas de Spoofing a interface de Loopback

-A LINWIZ-INPUT -s 127.0.0.0/8 -j DROP
-A LINWIZ-INPUT -d 127.0.0.0/8 -j DROP

-A LINWIZ-INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT

# Permite requisições de ICMP

-A LINWIZ-INPUT -p icmp -m icmp --icmp-type ping -j ACCEPT

# Permite os serviços autorizados

-A LINWIZ-INPUT -p tcp -m tcp --dport 20:21 -j ACCEPT
-A LINWIZ-INPUT -p tcp -m tcp --dport 25 -j ACCEPT
-A LINWIZ-INPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A LINWIZ-INPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A LINWIZ-INPUT -p udp -m udp --dport 53 -j ACCEPT

# Bloqueia o resto do tráfego

-A LINWIZ-INPUT -j REJECT-PKT

#######################################################################
# Resposta usada na rejeição do tráfego

-A REJECT-PKT -p tcp -m tcp -j REJECT --reject-with tcp-reset
-A REJECT-PKT -p udp -m udp -j REJECT --reject-with icmp-port-unreachable
-A REJECT-PKT -p icmp -m icmp --icmp-type ping -j REJECT --reject-with icmp-host-
unreachable

COMMIT
```

2.14 Portas padrão

Existe uma RFC (número 793) que padronizou a numeração das portas dos principais serviços na Internet. Essas portas também são conhecidas como "well-known ports". Na Tabela 2.4 listamos as principais portas apresentadas na RFC.

Tabela 2.4 – Portas padrão, conhecidas como "well-known ports"

Porta	Serviço
1	TCPMUX
5	Remote Job Entry (RJE)
7	ECHO
18	Message Send Protocol (MSP)
20	FTP – Data. File Transfer Protocol is a protocol used on the Internet for sending files.
21	FTP -- Control
22	SSH
23	TELNET
25	Simple Mail Transfer Protocol
29	MSG ICP
37	TIME
42	HOST NAME SERVER
43	WHOIS
49	LOGIN HOST PROTOCOL
53	DOMAIN NAME SERVER
69	TRIVIAL FILE TRANSFER PROTOCOL
70	GOPHER SERVICES
79	FINGER
80	HTTP
103	X.400
108	SNA GATEWAY ACCESS SERVER
109	POP2
110	POP3
115	SIMPLE FILE TRANSFER PROTOCOL
118	SQL SERVICES
119	NEWSGROUP NNTP
137	NETBIOS
139	NETBIOS DATA GRAM
143	IMAPS
150	NETBIOS SESSION SERVICE
156	SQL SERVICE
161	SNMP
179	BORDER GATEWAY PROTOCOL
190	GATEWAY ACCESS CONTROL PROTOCOL

Porta	Serviço
194	INTERNET RELAY CHAT IRC
197	DIRECTORY LOCATION SERVICES
389	LDAP
396	NOVEL NETWARE OVER IP
443	HTTPS
444	SIMPLE NETWORK PAGING PROTOCOL
445	MICROSOFT D-S
458	APPLE QUICKTIME
546	DHCP CLIENT
547	DHCP SERVER
563	SNEWS
1080	SOCKS

Vamos recapitular?

Neste capítulo foram apresentados os conceitos de bastion host e firewall, os principais tipos de firewalls, suas funcionalidades básicas e adicionais. No final do capítulo, apresentamos um caso de uso baseado no IP Tables.

Agora é com você!

1) O que o firewall stateful não consegue fazer?

2) Que tipo de firewall analisa apenas os endereços IP de origem e destino e as portas de origem e destino?

3) Qual o papel fundamental de um firewall?

4) Qual dispositivo de rede pode ser considerado um firewall?

5) Os firewalls são frequentemente utilizados para prevenir acessos não autorizados provenientes da Internet principalmente a:

   a) Intranet.

   b) Extranet.

   c) VPN.

   d) SMTP.

6) Qual equipamento trabalha como um procurador, recebendo solicitações de conexão e as executando ele mesmo no lugar da máquina original?

7) Qual o tipo de firewall que tem capacidade de inspecionar a camada de aplicação?

8) Qual é a porta de serviço do NetBios?

9) Qual o objetivo da DMZ?

10) Qual o número mínimo de interfaces de um firewall?

3

Firewalls de Nova Geração – NGFW

Para começar

Este capítulo apresenta os conceitos e o funcionamento de uma nova tecnologia introduzida em 2011, o Firewall de Nova Geração, ou NGFW. Esse equipamento traz uma série de benefícios e tecnologias capazes de expandir em muito o funcionamento de um firewall tradicional. Vamos detalhar ao longo do capítulo essa tecnologia.

3.1 O que é um Firewall de Nova Geração (NGFW)?

O primeiro ponto que devemos deixar claro: não se trata de uma nova tecnologia, mas sim do aprimoramento do firewall tradicional, ou seja, um Firewall de Nova Geração vai realizar todas as tarefas de um firewall tradicional mais uma série de novos recursos que o equipamento padrão não executa.

Inicialmente, o NGFW é um firewall de aplicação, ou seja, ele tem a capacidade que um IPS (Sistema de Prevenção a Intrusão) possui de fazer inspeção profunda nos pacotes. Com isso, consegue interpretar e entender o protocolo de aplicação e, a partir daí, permitir ou bloquear determinada aplicação. O interessante desse recurso é que o firewall é agnóstico à porta que a aplicação está utilizando, ou seja, mesmo que a aplicação trabalhe em uma porta não padrão, ela pode ser identificada. Muitos usuários com mais conhecimento configuram ou usam serviços em portas diferentes das portas padrão, as "well-known ports", como uma maneira de enganar o firewall.

Outro ponto é que o NGFW normalmente trabalha integrado a algum sistema de autenticação de usuários, como o AD (Diretório Ativo da Microsoft) ou o LDAP (usado em sistemas Linux/Unix).

Ou seja, por conta dessa integração, os NGFWs são capazes de saber qual usuário logado no sistema é o responsável por aquela conexão. Isso permite a criação de políticas específicas por usuário ou grupos.

Usando essas duas tecnologias podemos, por exemplo, permitir que determinado usuário tenha acesso à categoria de Redes Sociais e outro não. Na categoria de Redes Sociais no NGFW estarão todas as aplicações do tipo Facebook, LinkedIn, Twitter etc. O usuário João terá acesso, mas o usuário Pedro não, como observamos na Figura 3.1.

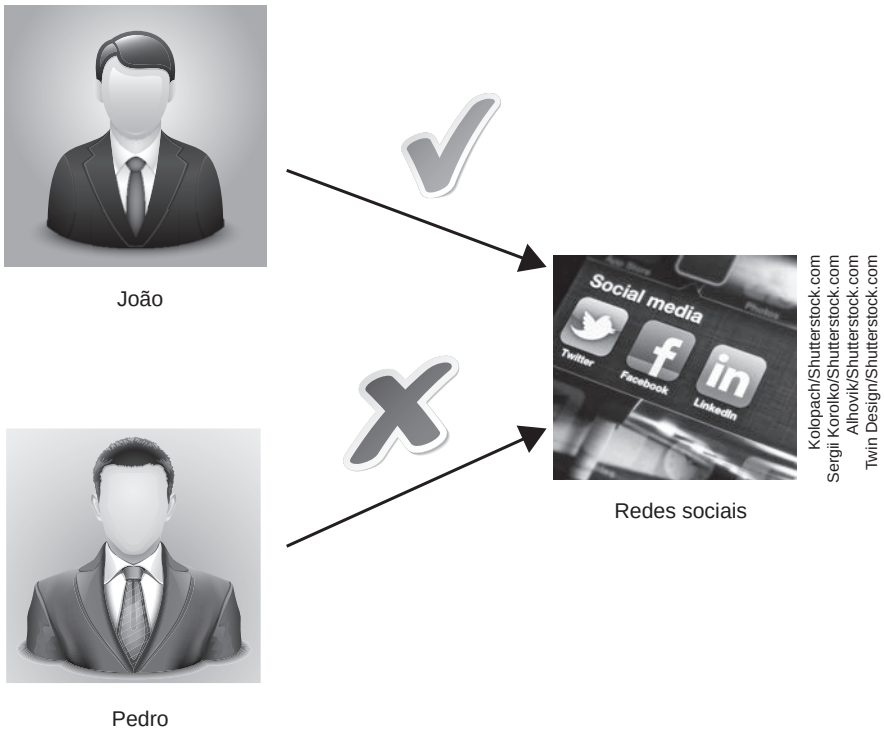


Figura 3.1 – Controle de Acesso por usuário.

O Firewall de Nova Geração também é agnóstico ao endereçamento IP, ou seja, quando definimos uma política por usuário, não importa o endereço IP que esse usuário esteja utilizando. O acesso pode ocorrer via VPN, pode ser sem fio e até via dispositivo móvel (smartphone ou tablet), mas a política tem que ser aplicada da mesma maneira. Isso é necessário nos dias de hoje, em que o perímetro da rede já não é tão bem delimitado.

Esses equipamentos são chamados de nova geração por agregarem mais inteligência e serviços avançados de detecção de ameaças não presentes em firewalls tradicionais. Os NGFWs já possuem intrínseca à sua arquitetura a funcionalidade de IPS (Intrusion Prevention System) integrada, com um grande conjunto de assinaturas para a detecção de ataques em tempo real. Além disso, esses equipamentos possuem chips capazes de realizar a decriptação em tempo real do tráfego encriptado que passa por eles, normalmente tráfego SSL, a partir da importação do certificado digital com a chave do servidor SSL interno. Esse recurso é muito importante, uma vez que boa parte do tráfego hoje em dia é baseada no uso de SSL, que, por ser encriptado, não consegue ser analisado pelos firewalls tradicionais.

Amplie seus conhecimentos

O que é SSL?

SSL é a sigla para Secure Software Layer. O SSL foi criado para trazer uma camada de segurança adicional principalmente aos protocolos de comunicação na web com o http. Ele torna possível o envio de tráfego encriptado, garantindo assim a confidencialidade das informações e a privacidade dos dados. Sem o SSL não seria possível realizarmos uma conexão segura com o banco para efetuar um pagamento ou colocarmos o número do cartão de crédito para uma compra segura em um site de comércio eletrônico.

alexwhite/Shutterstock.com

Figura 3.2 – SSL.

3.2 Serviço de IPS

Os serviços de prevenção de intrusão –(IPS), além de alertar sobre tentativas de ataque, permitem que elas sejam bloqueadas. Esse serviço realiza um nível de inspeção muito profunda no pacote, indo até a camada de aplicação do modelo OSI (camada 7). O IPS permite detectarmos os seguintes tipos de ameaças na rede, incluindo a rede sem fio:

- Propagação de vírus.
- Propagação de worms.
- Ataques direcionados a sistemas operacionais.
- Ataques direcionados a aplicações web, como cross site script, php injection e sql injection.
- Exploração de vulnerabilidades das principais aplicações.
- Spams e phishing.
- Spyware.
- Utilização da rede por aplicações não permitidas como P2P (incluindo Bittorrent).

Alguns benefícios da adoção do serviço de IPS:

- Redução das chamadas ao help desk: uma vez que esse serviço realiza o bloqueio das ameaças protegendo os dispositivos, em especial os computadores dos usuários, não há necessidade de uma ação do suporte para recuperar a máquina.
- Aumento do conhecimento e da visibilidade do tráfego da rede: esse serviço permite monitorar tráfegos e fluxos e identificar comportamentos anômalos que correspondam a alguma

atividade maliciosa. Assim, ele acaba atuando como um espião que consegue detectar tráfegos não esperados e não autorizados, como ataques internos, uso de aplicações não autorizadas como P2P (Emule, Bittorrent, entre outros), ataques de DoS (Negação de Serviço) e mesmo perda de dados, por meio de filtros de DLP (Data Loss Prevention).

» Controle de banda: um dos principais recursos do serviço de IPS é monitorar o uso de banda pelas aplicações e aplicar limitadores (Rate Limit). Esse recurso é essencial para o controle da rede e evita o seu mau uso. Vários clientes utilizam esse recurso para evitar congestionamentos na rede causados por streamings de vídeo e acessos a redes P2P. Temos como exemplo um cliente cujo IPS comprovou o uso de mais de 40% do link de comunicação com tráfego não permitido (P2P), aumentando os custos associados e, consequentemente, gerando lentidão nas aplicações válidas e essenciais à rede. Com o recurso de Rate Limit é possível definir um limite de banda para os tráfegos.

» Redução de custos com a recuperação de máquinas: sempre dizemos que é mais barata a prevenção que a remediação. Ataques bem-sucedidos em uma rede trazem prejuízos imensos às organizações, além de causar a indisponibilidade das máquinas, que ficam fora de operação até serem reinstaladas. O grande problema é a perda ou roubo dos dados contidos na máquina comprometida. A propriedade intelectual desses dados vale muitas vezes o valor da máquina, portanto, sua perda corresponde a um prejuízo muitas vezes incalculável. O rebuild de máquinas pode levar mais de duas horas por computador.

» Aumento da produtividade: computadores comprometidos geram tempo de parada e tempo de recuperação. Ambos podem ser muito grandes e representar uma diminuição na produtividade. Além disso, trabalhos salvos, mas que não possuíam backup, podem ter sido simplesmente perdidos quando a máquina foi comprometida, gerando novamente mais prejuízo. O serviço de IPS como elemento de proteção a esse tipo de ação é fundamental para o aumento da produtividade, reduzindo em 99% a quantidade de incidentes de segurança na rede.

» Outbreaks: a cada ano surge uma ameaça crítica que acaba gerando grandes problemas e indisponibilidades nas redes corporativas. Essas ameaças são conhecidas como "outbreaks". O grande último outbreak por que passamos foi o Conficker, um worm que se propagava rapidamente na rede derrubando o serviço de DNS interno e congestionando o serviço de autenticação do Windows (Active Directory). Usuários que acreditavam que os sistemas de antivírus e o firewall fossem capazes de bloquear a ameaça foram surpreendidos pela paralisação total da rede. Alguns worms críticos são capazes de infectar toda a rede em poucos minutos.

» Patch virtual: o serviço de IPS atua como um patch virtual. Normalmente, é necessário muito tempo para se atualizar todo o parque de máquinas quando uma nova ameaça é conhecida. Assim, muitas vezes a gerência de TI acaba deixando para realizar as atualizações nos finais de semana, quando já é tarde demais. O IPS instalado na rede atua como um patch virtual, uma vez que mesmo que as máquinas estejam vulneráveis qualquer tentativa de explorar a vulnerabilidade será bloqueada pelo IPS, protegendo-se assim as estações.

» Web application firewall: é notória a dificuldade que muitas vezes enfrentamos para alterar uma aplicação e torná-la menos vulnerável. Nesse caminho, frequentemente é muito mais barato bloquear pela rede as ameaças a um sistema do que realizar as correções na

aplicação. Nesse ponto, o serviço de IPS acaba sendo um instrumento fundamental para proteger as aplicações, especialmente aplicações web.

» Proteção de infraestrutura de voz sobre IP: as reduções de custos atreladas ao uso da voz sobre IP são uma realidade no ambiente de TI de uma organização moderna. Entretanto, esse ambiente é vulnerável a uma série de ataques cujo objetivo seja indisponibilizar o serviço ou mesmo a realização de chamadas não autorizadas. Nessa linha, o IPS tem uma completa cobertura de vacinas que protege contra ataques à infraestrutura VoIP.

3.3 Serviços avançados – Sandbox

Com o crescimento das ameaças e os ataques se tornando mais inteligentes, é necessário que os dispositivos de segurança estejam preparados para lidar com cenários cada vez mais espinhosos. Hoje, os hackers utilizam técnicas conhecidas como APT (Advanced Persistent Threats, ou ameaças persistentes).

As APTs exploram muitas vezes vulnerabilidades de Dia Zero (ainda não conhecidas, portanto, os sistemas estão desprotegidos contra elas) e se caracterizam por ataques realizados em um longo espaço de tempo, de forma a dificultar a sua detecção por ferramentas tradicionais.

Muitos desses ataques se iniciam com o envio de e-mails falsos, como spams, com arquivos infectados anexados. Esses arquivos podem estar em diferentes formatos, incluindo extensões que normalmente não são consideradas ameaças, como .pdf, .docx e .xlsx. A maior parte desses arquivos está infectada por malwares (códigos maliciosos), que dificilmente são identificados por antivírus tradicionais.

Esse código malicioso tem como característica a capacidade de alterar o próprio código, dificultando assim a sua detecção por sistemas de antivírus focados em assinaturas. A detecção dessas ameaças envolve o uso de novas tecnologias, como o Sandbox.

A tecnologia de Sandbox é algo novo que agrega recursos de virtualização com detecção avançada de ameaças. Basicamente, essas ferramentas ficam "escutando" o tráfego de rede, e, quando detectam a transmissão de um arquivo, ele é capturado e enviado para teste no ambiente de Sandbox.

Nesse ambiente existem diversas máquinas virtuais equipadas com diferentes versões de diferentes sistemas operacionais. Normalmente, são configuradas para funcionar nas versões existentes de sistemas operacionais existentes na rede. Por exemplo, se a empresa utiliza Microsoft Windows Server 2008, Linux CentOS e Windows 7, essas máquinas devem estar presentes para a realização dos testes de Sandbox.

Os arquivos são testados no ambiente virtual, isto é, são executados nessas máquinas, e a ferramenta detecta se apresentam algum comportamento fora do que seria esperado.

Caso seja detectada alguma anomalia no processamento - por exemplo, alterações no registro da máquinas, acesso a endereços ou páginas de má reputação, tentativa de estabelecimento de conexões para vários destinos na Internet que possam caracterizar o estabelecimento de um canal de comando (comunicação) com a máquina do hacker, aumento do uso de recursos como memória, cpu e I/O, temos indícios de que a ameaça está presente, o arquivo está infectado por algum tipo de malware e precisa ser isolado, ou seja, a solução deve tomar ações de bloqueio para conter a ameaça.

Esse processo muitas vezes requer a adição de um módulo específico de segurança que é executado fora do NGFW. Em muitos fabricantes, trata-se de um servidor externo, conhecido como ATA (Advanced Threat Analysis, ou detector de ameaças avançadas).

A tecnologia de Sandbox é atualmente a que mais cresce em utilização, sendo requerida por grandes corporações devido principalmente ao declínio da detecção de ameaças pelos sistemas de antivírus tradicionais. Na maior parte das empresas em que se testa essa tecnologia percebe-se que já há infecção há muito tempo, sem que houvesse detecção pelos sistemas de antivírus.

Alguns fabricantes vêm investindo bastante nessa tecnologia, como a TrendMicro, a HP, a FireEye e a McAfee.

3.4 Serviços avançados de reputação

Os serviços de reputação são um recurso muito importante para detectar ameaças. Esse serviço permite analisarmos a origem das conexões e verificar sua reputação (se boa ou má). Normalmente, as informações são atualizadas várias vezes ao dia e nos permitem verificar a reputação de:

» Arquivos: refere-se a arquivos que normalmente são enviados via internet e cujo hashing (assinatura que permite verificar se o arquivo foi modificado) já tenha sido calculado.

» Domínios na Internet: verifica se estamos recebendo conexões provenientes de domínios com má reputação. Essa técnica é muito utilizada para detectar mau uso da rede por usuários da rede interna que eventualmente acessem, por exemplo, conteúdos não permitidos, como sites de jogos.

» Endereços IP: essas listas possuem milhares de endereços IP de má reputação.

Normalmente, os serviços de reputação nos permitem verificar uma série de condições a partir da definição de um nível de pontuação. Esse nível de pontuação vai de 0 a 100, permitindo definir o que é mais e o que é menos crítico. Itens próximos de 100 representam o nível mais alto de risco, e, a partir daí, devemos definir um nível no qual monitoramos a conexão (normalmente, acima de 50) e um nível no qual bloqueamos a conexão maliciosa (normalmente, acima de 70).

As principais ameaças categorizadas pelos serviços de reputação são:

» BotNets: no caso de a origem ser ou fazer parte de uma BotNet, o que pode representar um grande risco. Afinal, uma máquina membro de uma BotNet pode ser acessada remotamente por um hacker e trazer uma ameaça extremamente crítica para a empresa.

» Worm: esses endereços relacionam origens que estão infectadas por um worm e que, portanto, podem propagar uma infecção pela rede. O worm tem como característica a autorreplicação, e seus efeitos podem ser devastadores na rede. Algumas infecções por worm, como o Conficker, trouxeram grandes prejuízos às empresas.

» Vírus: nessa categoria estão as origens que hospedam vírus ou que já foram responsáveis por infecções por vírus. Os vírus normalmente se propagam em arquivos infectados, que devem ser executados para o vírus se replicar.

» Atacantes a servidores web: esses endereços são de origens que realizam ataques a servidores e aplicações na web. São cadastrados na lista de reputação porque a ideia é bloquear as conexões provenientes dessas origens.

» Spam: essa categoria tem como objetivo bloquear usuários que enviam spams constantemente. Esses endereços e domínios estão presentes nas listas de reputação, que podem ser utilizadas como uma importante ferramenta de bloqueio.

3.5 Geolocation (localização geográfica)

Esse serviço permite que criemos políticas específicas para monitorar e bloquear conexões oriundas de determinada região ou país. A ideia é que podemos ter um mecanismo para agregar essas informações à política do firewall.

Um exemplo da utilização desse recurso ocorreu alguns anos atrás, quando hackers do Anonymous realizaram ataques em massa, muitos deles de negação de serviço nos Estados Unidos. A maioria dos ataques era originária de fora do país, e para deles se defender, muitas empresas incluíram em suas políticas de segurança uma configuração conhecida como "patriota". Essa configuração bloqueava, durante o período do ataque, conexões provenientes de países que não fossem os próprios Estados Unidos. Foi uma ação deveras radical, mas que fazia sentido no cenário de ataques que estava ocorrendo.

3.6 Integração com sistemas de autenticação

Os NGFWs possuem integração nativa com os sistemas de diretório ativos, ou seja, eles conseguem de forma transparente identificar os usuários que estão logados no sistema. Essa informação pode ser usada tanto na definição de políticas como na informação forense dos logs de acesso.

Esse recurso é muito interessante porque podemos definir uma política de firewall independentemente de qual endereço IP o usuário utilizou. Isso envolve um novo conceito, por conta dos diferentes tipos de acesso que possuímos hoje: por VPN, por rede sem fio, via smartphones e tablets etc. Ou seja, os usuários acabam acessando as redes com diferentes endereços e por diferentes dispositivos, o que dificulta a implantação de uma política baseada em endereços. Quando mudamos esse paradigma para uma política por usuário, chegamos a uma solução mais personalizada e de fácil gestão.

leungchopan/Shutterstock.com

Figura 3.3 – Sistemas de autenticação.

3.7 Recursos de VPN

Um firewall de nova geração deve possuir os mesmos recursos de VPN de um firewall tradicional. Normalmente, esses firewalls permitem implementar dois serviços de VPN, o IPSEC (usando um cliente de VPN) e a VPN SSL (sem cliente).

3.7.1 VPN IPSEC

3.7.1.1 IPSec

Baseado na RFC 2401, o IPSec foi implementado para operar tanto em um ambiente de estação do usuário como em gateway (roteador, concentrador etc.), garantindo a proteção para o tráfego IP. A proteção oferecida é baseada nas necessidades da política de segurança estabelecida e mantida pelo usuário ou administrador do sistema.

O IPSec é um protocolo de tunelamento desenhado tanto para IPv4 como para IPv6, e disponibiliza segurança fim a fim entre redes IP.

O IPSec disponibiliza mecanismos de segurança e criptografia na camada IP.

Basicamente, os seguintes serviços são disponibilizados:

» Integridade dos dados: os pacotes são protegidos contra modificação acidental ou deliberada.

» Autenticação: a origem de um pacote IP é autenticada criptograficamente.

» Confidencialidade: a parte útil de um pacote IP ou o próprio pacote IP pode ser criptografada(o).

» Antirreplay: o tráfego IP é protegido por um número de sequências que pode ser usado pelo destino para prevenir ataques do tipo replay (repetir a mesma sequência antes enviada).

O IPSec permite a interoperabilidade de implementações de diferentes fabricantes e é uma solução de segurança fim a fim entre roteadores, firewalls, estações de trabalho e servidores. O IPSec se integra de forma transparente com a pilha TCP/IP existente, sendo transparente para todas as aplicações, ou seja, não há necessidade de executar nenhuma alteração nos sistemas existentes para a aplicação do IPSec.

O IPSec utiliza criptografia simétrica, devido à rapidez do mecanismo para encriptar os dados, e criptografia assimétrica para prover mecanismos de troca de chaves criptográficas. Conforme já discutimos neste capítulo, os algoritmos de hashing no IPSec geram hashings de tamanho de 128 ou 160 bits.

Algoritmos suportados pelo IPSec:

» Criptografia: AES, DES, 3DES, RC5, IDEA, CAST e Blowfish.

» Hashing: MD5, SHA-1 e Tiger.

» Autenticação: assinaturas digitais RSA e assinaturas digitais DSS.

3.7.1.2 Associação de segurança

É um acordo estabelecido entre os dois pontos da comunicação para negociação de parâmetros do túnel IPSec. Esse acordo deve ser estabelecido antes da criação do túnel IPSec. Entre os mesmos dois pontos podem existir múltiplas associações de segurança.

As associações de segurança ficam armazenadas na SPD ("Security Policy Database", ou base de dados da política de segurança) e na SAD ("Security Association Database"). Cada associação de segurança possui seu identificador único, identificado pelo SPI ("Security Parameter Index").

Na associação de segurança são negociados os seguintes mecanismos de segurança:

» Modo do túnel IPSec: ESP ou AH.
» Algoritmo de criptografia.
» Método de autenticação.
» Função de hashing.
» Método de autenticação do usuário: RADIUS, SecurID.
» Escolha das chaves criptográficas e chaves de autenticação.

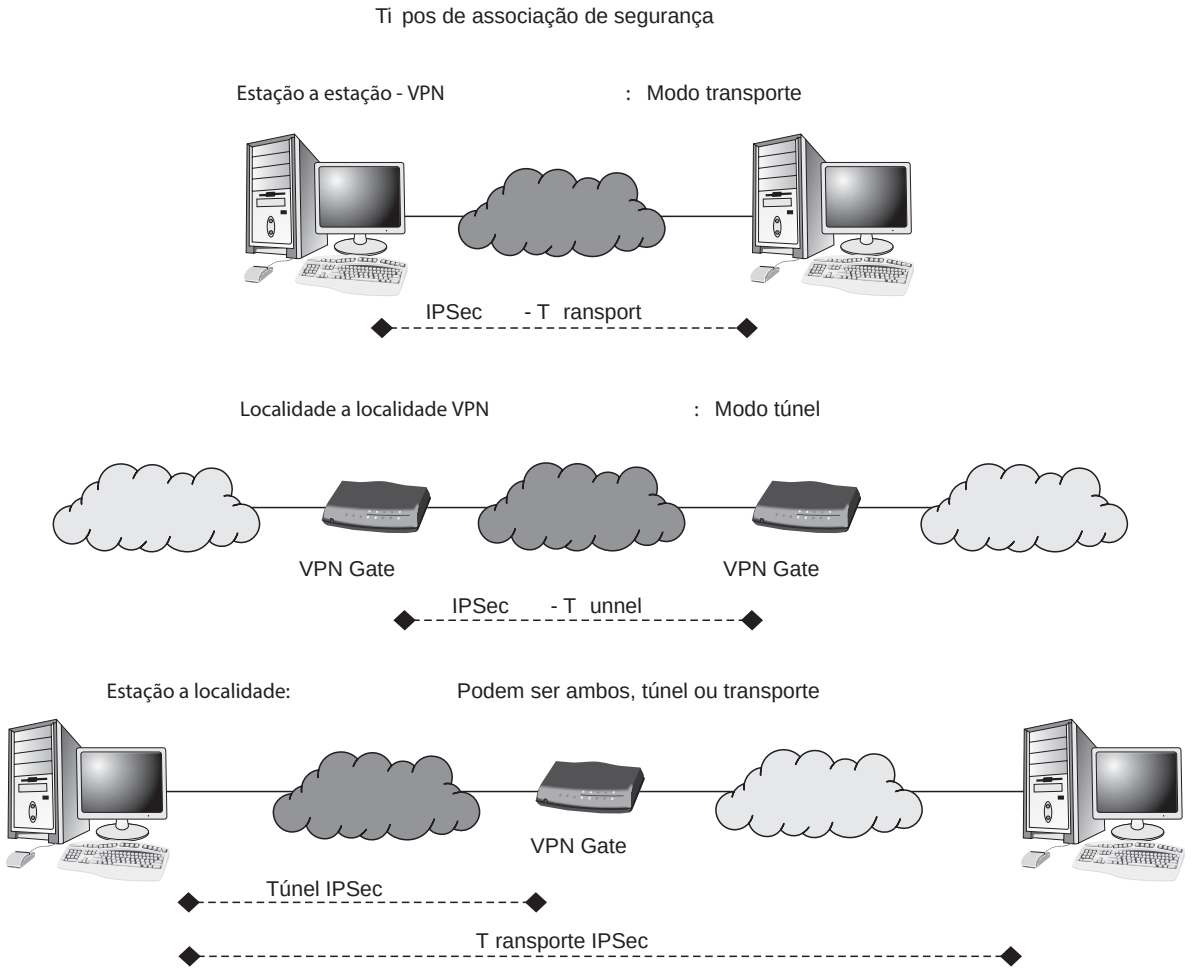


Figura 3.4 – VPN IPSec – Modos.

O IPSEC nos permite criar dois modos de VPN:

» Client to Server: nesse modo, uma máquina com um cliente de VPN pode se conectar ao NGFW (servidor de VPN).

» Server to Server: esse modo pode ser observado na Figura 3.4, em que um NGFW servidor se conecta a outro NGFW servidor.

3.7.2 VPN SSL

Há alguns anos foi criada essa tecnologia, que permite a criação de um VPN sem o uso de um cliente IPSEC instalado.

Nesse processo, precisamos apenas abrir uma página web hospedada no NGFW e clicar em um ícone para que um componente em JAVA seja executado. O próximo passo é informar usuário e senha para se autenticar na VPN.

A VPN é estabelecida por meio de um túnel criado sobre a conexão SSL. A única necessidade do usuário é que se mantenha a janela aberta.

Os protocolos da pilha TCP/IP podem ser encapsulados nesse túnel, garantindo-se assim a conectividade.

3.8 Alta disponibilidade

Existem alguns modos de implementação de um NGFW. Normalmente, quando utilizamos esses equipamentos em grandes clientes, uma das maiores preocupações é o que vai ocorrer com a rede se eles falharem, principalmente porque o NGFW está na borda da rede e, se houver falha, toda a rede fica fora do ar.

Uma das opções na implementação de um firewall é usar um serviço de Alta Disponibilidade, que consiste em alocar um segundo firewall de mesma capacidade para trabalhar de forma paralela e em cluster ao firewall principal.

Esse cluster pode ser Ativo-Ativo (desse modo, se um dos firewalls der problema o outro assume) ou Ativo-Passivo (no modo Ativo-Passivo, o segundo firewall fica dormindo e assume quando ocorrer alguma falha no primeiro firewall).

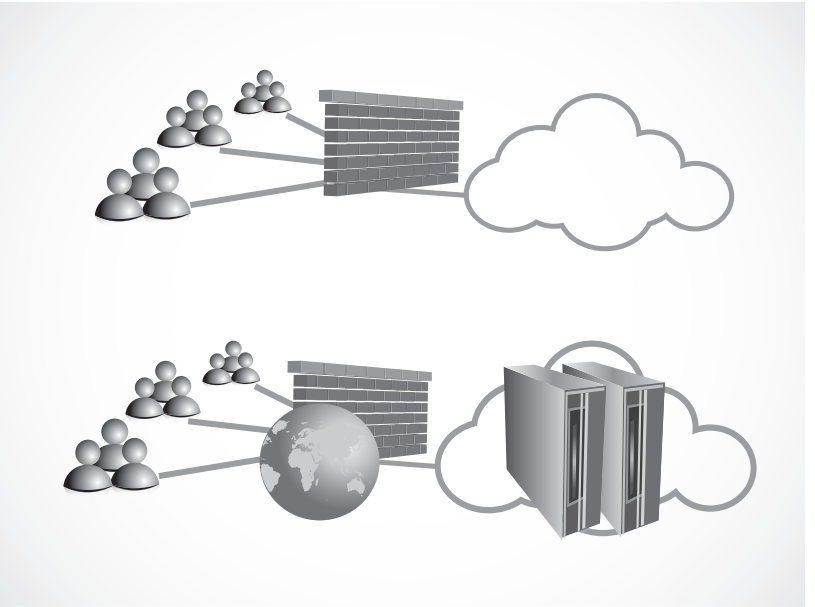


Figura 3.5 – Firewall em alta disponibilidade Ativo-Passivo.

Vamos recapitular?

Neste capítulo apresentamos a nova geração de firewalls, os chamados NGFWs, bem como suas capacidades avançadas se comparadas às de um firewall tradicional, como inspeção de SSL, controle de acesso por usuário, serviço de IPS, serviço de Sandbox, serviços avançados de reputação, geolocation e recursos de VPN.

Agora é com você!

1) Quais as principais vantagens de um Firewall de Nova Geração?

2) O que é uma APT ("Advanced Persistent Threat")? No que consiste o serviço de geolocalização?

3) Qual o objetivo da tecnologia de Sandbox?

4) Como podemos comparar as tecnologias de VPN IPSEC e SSL VPN?

5) Como o serviço de reputação pode nos auxiliar na detecção de ameaças? Cite três categorias que podem ser bloqueadas por esse serviço.

6) O que é a tecnologia de IPS ("Sistemas de Prevenção a Intrusão") incorporada à tecnologia dos NGFWs?

7) Qual a vantagem da criação de políticas por usuário? Exemplifique como podemos explorar esse recurso.

8) O processo de utilização de tecnologia de Sandbox envolve escolher inicialmente quais máquinas virtuais devem ser selecionadas para testar os arquivos. Qual o critério que devemos escolher para selecionar essas máquinas?

9) Que tipo de ameaça um NGFW consegue bloquear, mas um firewall tradicional não?

4

Introduzindo o Microsoft ISA Server

Para começar

Neste capítulo vamos fazer uma breve revisitada no Microsoft ISA Server. Entenderemos como a arquitetura funciona e visitaremos as principais telas e funcionalidades do ISA Server.

4.1 O que é o Microsoft ISA Server

Primeiro vamos entender o que significa ISA (Internet Security and Acceleration Server), ou seja, um servidor capaz de prover segurança e aceleração no acesso, ou seja, estamos falando de cache e de um servidor de Proxy. Essa solução é a evolução de um outro produto da Microsoft chamado Microsoft Proxy Server 2.0.

O ISA nada mais é do que um firewall que pode trabalhar a nível de pacote, circuito ou aplicação, associado a recursos de cache de páginas Internet. Existe uma grande quantidade de usuários que utiliza o ISA muito mais como um cache de páginas Internet do que um firewall.

O nome aceleração vem justamente do recurso de cache Internet que nos permite armazenar localmente páginas. Essas páginas uma vez que são acessadas ficam armazenadas no cache do ISA e o próximo acesso é realizado diretamente do ISA e não da Internet, aumentando a velocidade do processo e diminuindo o tráfego Internet.

Como o ISA server trabalha integrado ao diretório ativo do Windows, é possível controlar usos e políticas por usuário, grupo, aplicação e destino. Ele trabalha com o protocolo de autenticação Kerberos.

4.1.1 O que é o Kerberos?

O Kerberos é um protocolo de autenticação seguro definido pela RFC 1510. O Kerberos foi desenvolvido no projeto Athena do MIT (Massachusetts Institute of Technology).

Essa é uma solução madura, confiável e segura para autenticação de rede. Esse protocolo é baseado no uso de tecnologia de criptografia de chave simétrica, ou chave secreta; além disso, é o protocolo de autenticação nativo do sistema operacional Microsoft Windows 2000 em diante.

Esse protocolo usa um processo de requisição de tíquete encriptado para a autenticação. Esse tíquete é usado para uma requisição em particular de um servidor. Nesse processo é o tíquete que é enviado pela rede e não a senha do usuário.

Resumidamente, o Kerberos funciona da seguinte forma: suponha que você deseja acessar um servidor em outro computador, e você saiba que esse servidor necessita de um tíquete Kerberos para atender a sua requisição.

Para conseguir esse tíquete você deve inicialmente requerer autenticação do servidor de autenticação AS do Kerberos. Esse servidor por sua vez criará uma chave de sessão baseada não sua senha e um valor randômico que representa o serviço requisitado. A chave de sessão é efetivamente um TGT "ticket-granting ticket".

Agora de posse do TGT você deve enviá-lo ao ticket-granting server (TGS). O TGS retorna então o tíquete que deve ser enviado ao servidor para requisitar o serviço.

O servidor pode aceitar ou rejeitar o tíquete.

Como o tíquete possui um carimbo de tempo, ele permite que o usuário utilize aquele tíquete apenas por determinado tempo, passado esse tempo ele deve ser reautenticado.

Para ficar mais claro, vamos imaginar que existem duas personagens, muito usadas em sistemas criptográficos: o Bob e a Alice. Alice é o cliente que deseja obter múltiplas autenticações no servidor que é o Bob.

Inicialmente, pelo processo de autenticação do Kerberos, Alice deve obter um bilhete de autenticação chamado de TGT (Ticket Granting Ticket) em um servidor de bilhetes que faz parte do sistema de autenticação chamado TGS (Ticket Granting Service).

De posse desse bilhete, Alice envia o mesmo ao servidor (Bob) para obter um novo bilhete chamado de Bilhete de Serviço. Esse bilhete é então novamente apresentado a Bob na forma criptografada para autenticar Alice. A Figura 2.1 ilustra bem o processo de troca de informações de autenticação entre Alice (Cliente) e Bob (servidor):

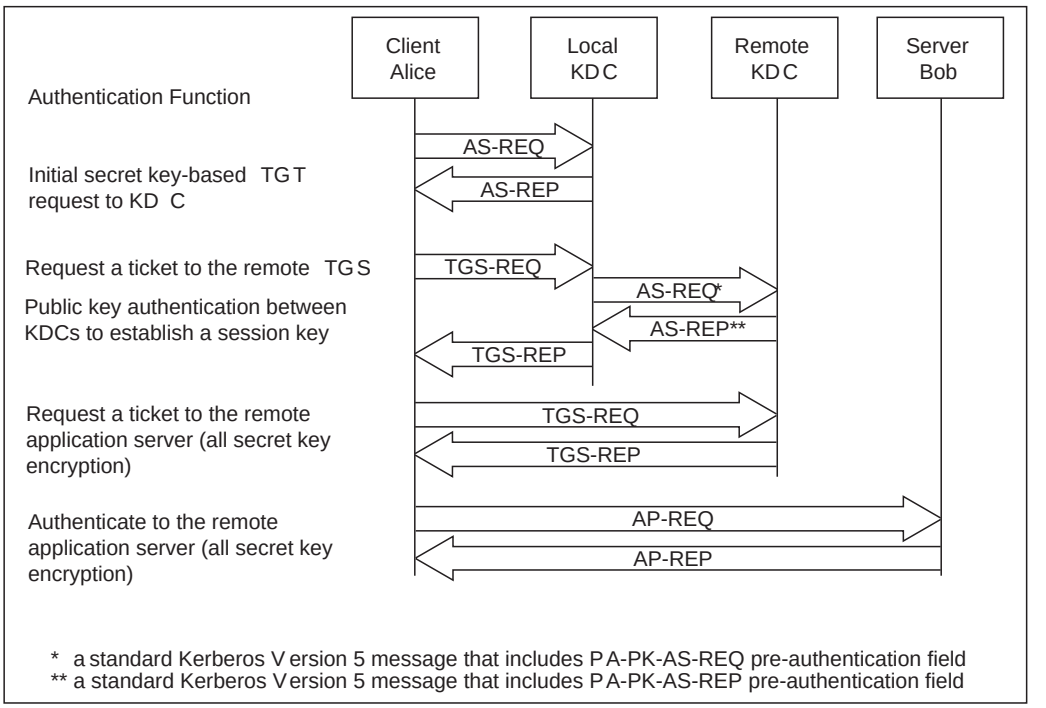


Figura 4.1 – Kerberos: troca de informações de autenticação entre Alice e Bob.

4.2 Arquitetura do ISA Server

O ISA Server nos permite uma série de recursos, entre eles:

» Integração do com diretório ativo (AD): o gerenciamento do ISA é facilitado pela integração com o sistema de Diretórios do Microsoft Server.

» Múltiplos métodos de autenticação: o ISA Server suporta os seguintes métodos de autenticação: básico, Digest, NTLM, Kerberos, e certificados digitais, Active Directory, RADIUS, ou SecurID Authentication Manager.

» Sistema operacional protegido: os serviços não utilizados no servidor ISA são desabilitados, aumentando a proteção da mesma.

» VPN: o ISA Server pode ser utilizado como um concentrador de VPN, suportando protocolo como o L2TP, IPSec e o PPTP.

» NAT (Network Address Translation): esse recurso permite que o ISA implemente NAT para dentro da rede.

4.3 Regras de segurança do ISA Server

O pacote quando chega no ISA Server, ele segue uma sequência: inicialmente são aplicadas regras de filtro de pacotes, em seguida são analisadas as regras de publicação Web, as regras de roteamento e por último as regras de controle de banda. Quando o pacote sai do ISA, o processo segue na ordem inversa.

4.3.1 Filtro de pacote

As regras de filtro de pacotes garantem que se não existe uma política específica que trata determinado tráfego este deverá ser negado por padrão. Os filtros de pacotes podem ser configurados para permitir ou negar a maior parte dos tráfegos da rede externa para rede interna.

Os filtros de pacotes normalmente são implementados sobre pacotes TCP, mas também podem ser criadas regras para UDP e ICMP. Os filtros contêm informações de endereços origens e destinos e as portas de comunicações aplicadas. Normalmente trabalhamos com as well-know ports definidas na RFC 1700, que pode ser obtida no site <https://www.ietf.org/rfc/rfc1700.txt>. O ISA Server, portanto, bloqueia as aplicações baseadas nas portas que as mesmas utilizam.

As well-known ports podem ser consultadas também na Tabela 2.4 deste livro.

4.3.2 Filtro de web

Nessas regras temos configuradas as políticas de cache e as políticas de acesso às páginas web. É possível também trabalhar com o proxy reverse, que veremos em detalhes no Capítulo 6.

4.3.3 Regras de roteamento

As regras de roteamento indicam qual requisição deverá ser roteada ou redirecionada a outro servidor. Normalmente, se possuímos alguma página que está no cache esse direcionamento pode não ocorrer.

4.3.4 Regras de banda

É possível implementar funcionalidades de QoS (qualidade de serviço) no ISA Server, podendo assim controlar o acesso à Internet dos usuários.

4.3.5 Políticas de protocolos

A ideia dessas políticas é definir os protocolos que serão utilizados, podendo portanto os mesmos ser permitidos ou bloqueados pelo ISA. Os protocolos que trabalhamos no ISA quando estamos em cache são HTTP, HTTPS, FTP e Gopher.

4.3.6 Regras de conteúdo e sites

São as regras de acesso a sites e conteúdos, como uma URL específica. Essas regras podem inclusive ser definidas em grupo.

4.4 Instalando o ISA Server 2006 para Windows

É muito importante analisar os requisitos para a instalação do pacote. Segundo o próprio site da Microsoft, é necessário que um computador disponha, no mínimo, desses requisitos básicos para instalação:

- Processador de 733 MHz Pentium III ou superior.
- Sistema operacional mínimo Microsoft Windows Server 2003 32-bit com Service Pack 1.
- Memória de 512 megabytes (MB) de RAM.

» Disco rígido formatado com NTFS e pelo menos 150MB de espaço disponível.

» Placas de rede necessárias compatíveis com o Windows.

» 1.º passo: baixe o arquivo de instalação.

O primeiro passo para instalação é baixarmos o pacote, que pode ser encontrado no link: <http://www.microsoft.com/pt-br/download/details.aspx?id=15244>.

Lembramos que o Windows é um software proprietário da Microsoft e que possui licenciamento. Nesse site é possível baixar um pacote de avaliação por um tempo limitado, apenas para testar a ferramenta.

» 2.º passo: execute o arquivo de instalação.

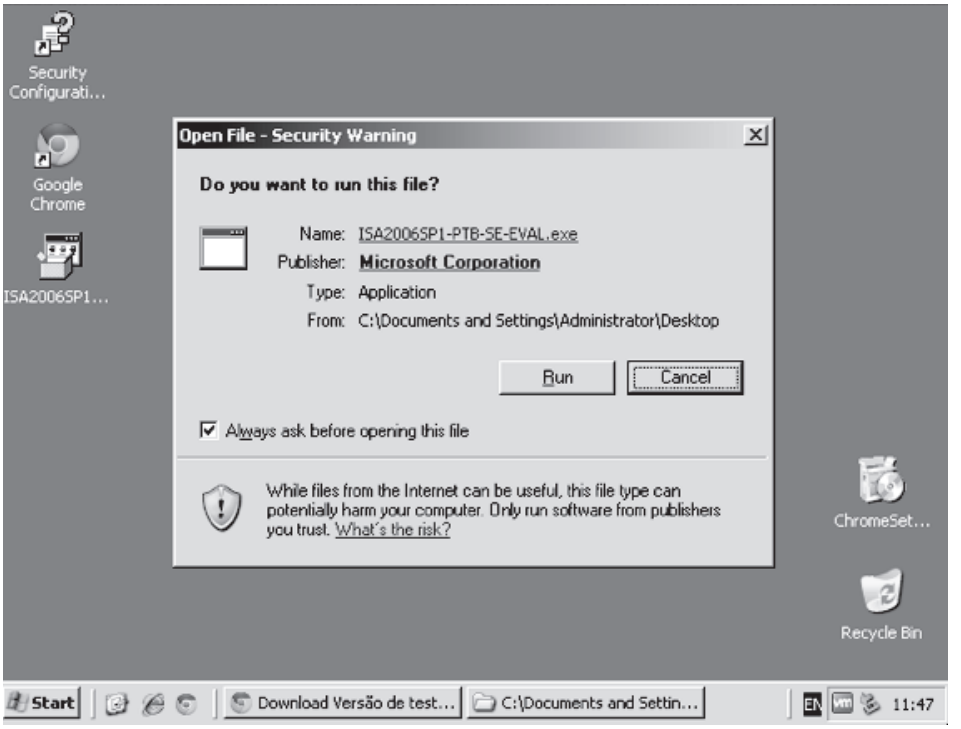


Figura 4.2 – Tela inicial de execução do arquivo.

Clique em Run ⇒ Executar.

» 3.º passo: confirme a instalação.

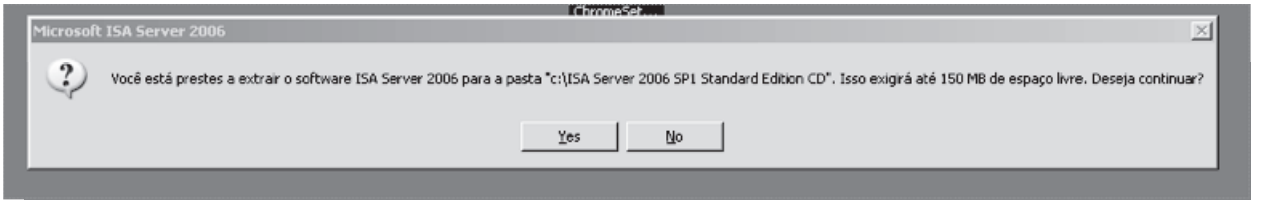


Figura 4.3 – Tela de confirmação da instalação.

Clique Yes (Sim, no Windows em português).

4.º passo: tela inicial para a instalação.

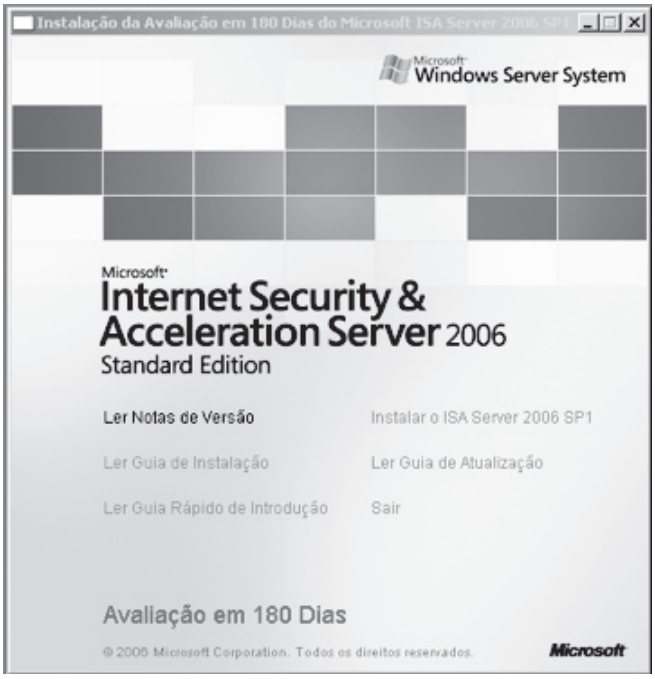


Figura 4.4 – Menu inicial de instalação.

Clique em Instalar o ISA Server 2006 SP1.

» 5.º passo: clique em Avançar para prosseguir a instalação.

Figura 4.5 – Assistente de instalação.

» 6.º passo: aceite a licença.

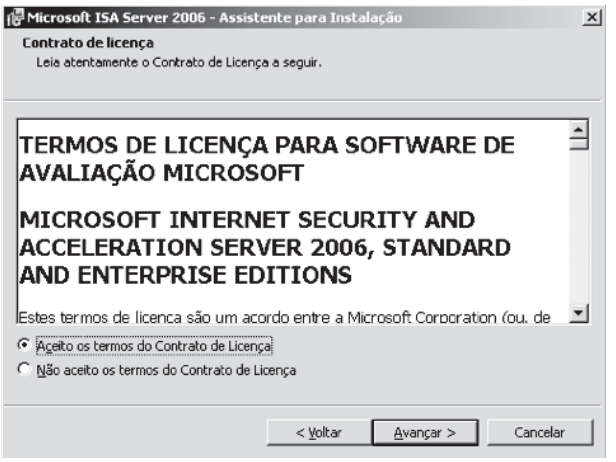


Figura 4.6 – Aceitar a licença.

Clique em Avançar.

» 7.º passo: confirme a licença de avaliação.

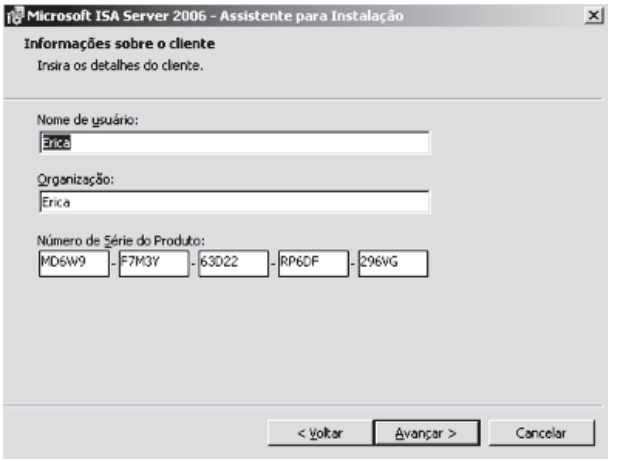


Figura 4.7 – Licença de avaliação.

Clique em Avançar.

» 8.º passo: escolha a instalação típica.

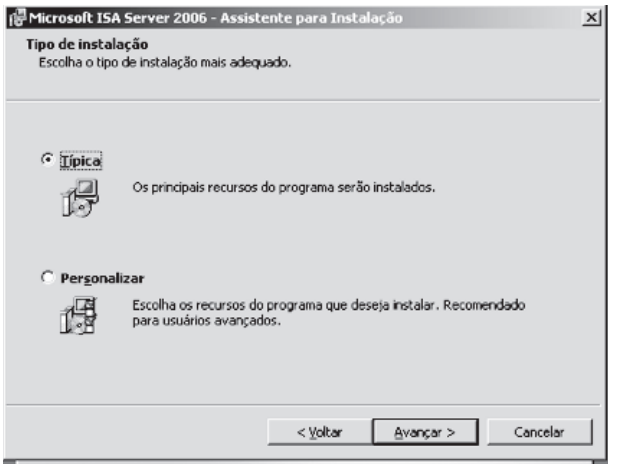


Figura 4.8 – Escolhendo a instalação típica.

Clique em Avançar.

» 9.º passo: associe a interface para Rede Interna.

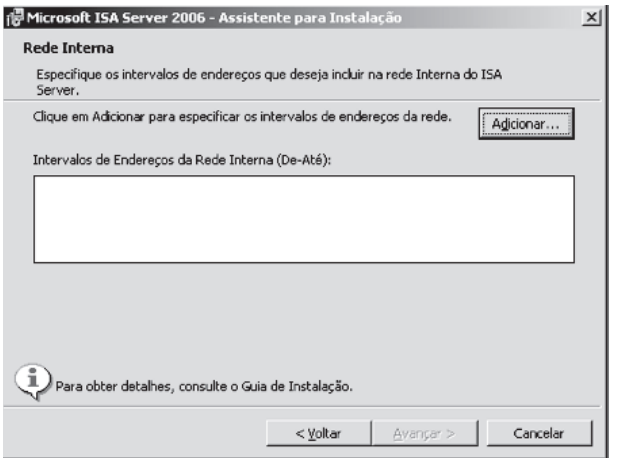


Figura 4.9 – Adicionando interface de Rede Interna.

Clique em Adicionar.

» 10.º passo: escolha uma das interfaces da máquina para rede interna.

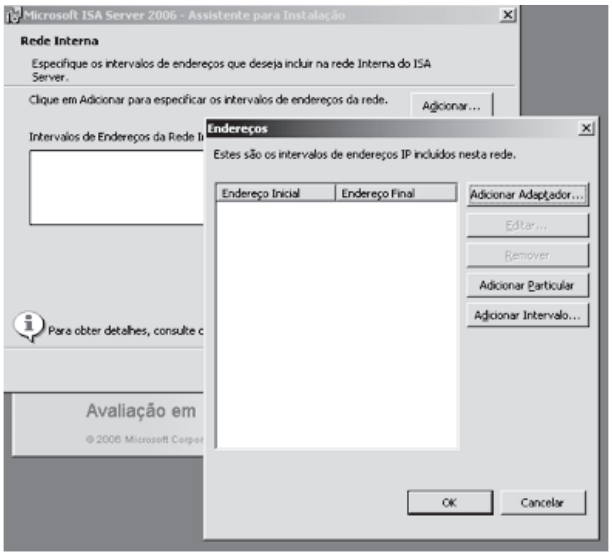


Figura 4.10 – Adicionando a interface.

Clique em Adicionar Adaptador.

» 11.º passo: escolha o adaptador.

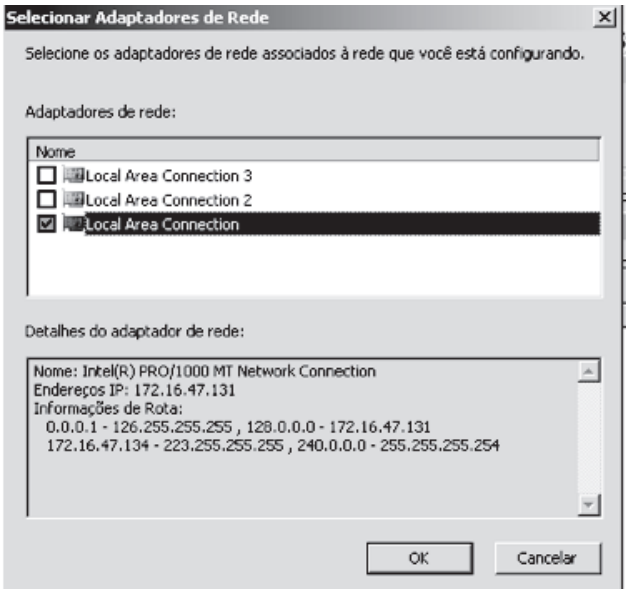


Figura 4.11 – Selecionando a interface de rede local.

Clique em OK.

» 12.º passo: Clique em OK.

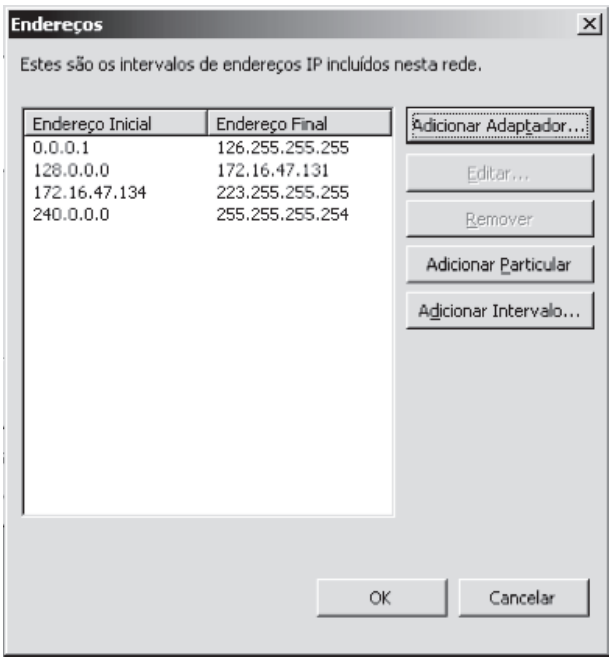


Figura 4.12 – Confirmando a interface.

» 13.º passo: Clique em Avançar.

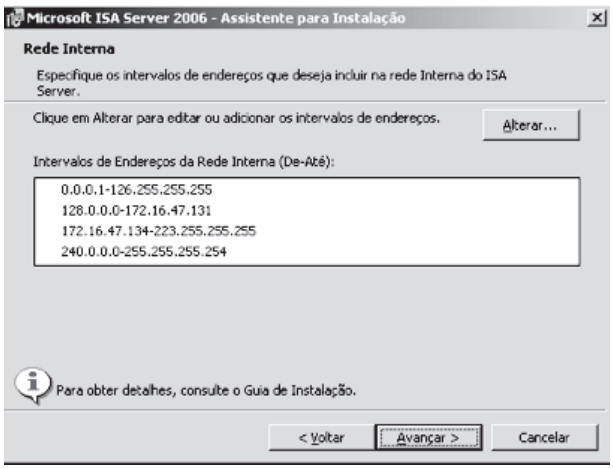


Figura 4.13 – Confirmando a instalação.

» 14.º passo: selecione a opção Permitir conexões não criptogradas.

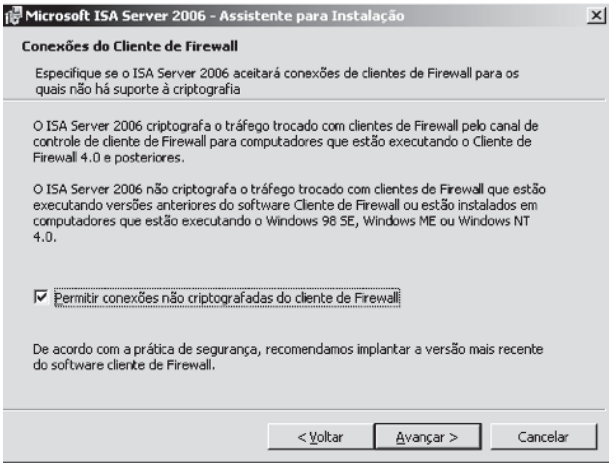


Figura 4.14 – Selecionar que permite conexão não encriptada.

» 15.º passo: confirme a conclusão e Avançar.

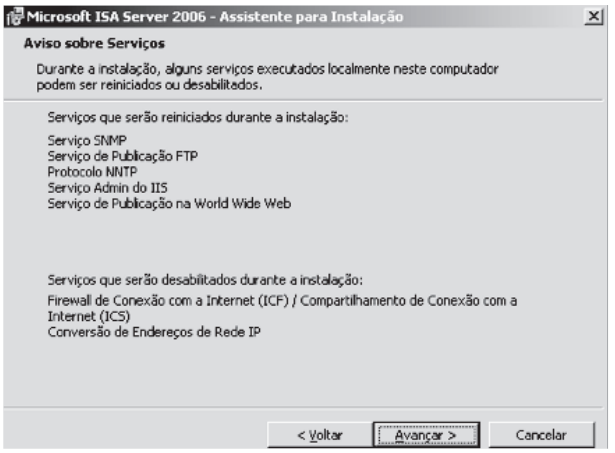


Figura 4.15 – Prosseguindo com a instalação.

» 16.º passo: clique em Instalar, para iniciar a instalação.

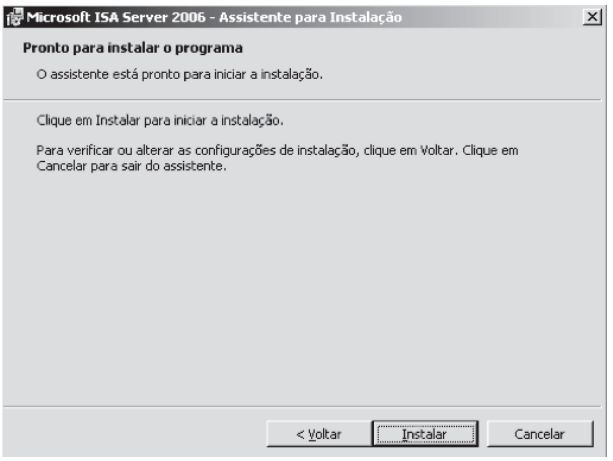


Figura 4.16 – Iniciando a instalação.

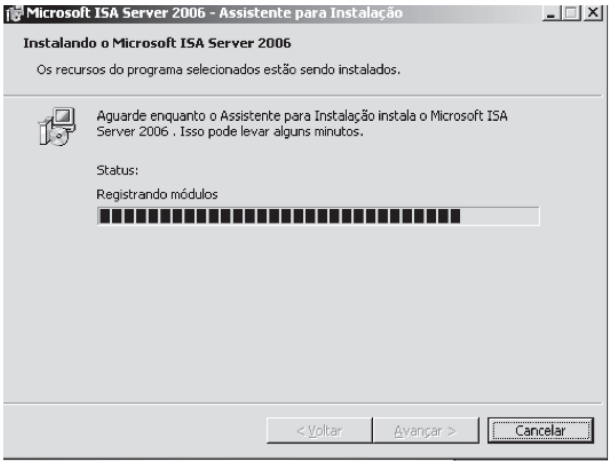


Figura 4.17 – Andamento da instalação.

Em seguida, você verá a instalação em execução.

» 17.º passo: Instalação Concluída – clique na opção “Invocar o gerenciamento” após o término.

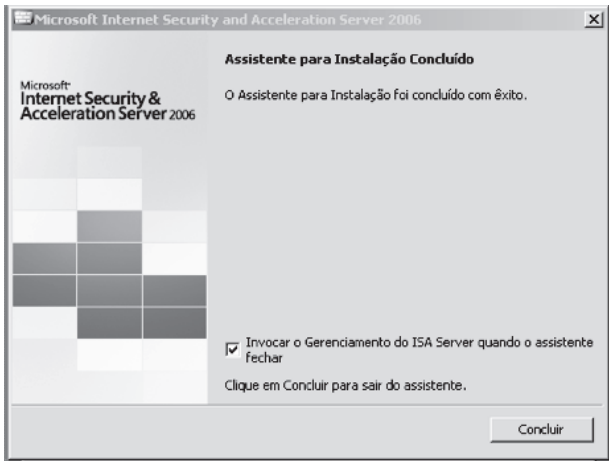


Figura 4.18 – Concluindo a instalação.

Clique em Concluir.

» 18.º passo: a Console do ISA Server deverá abrir.

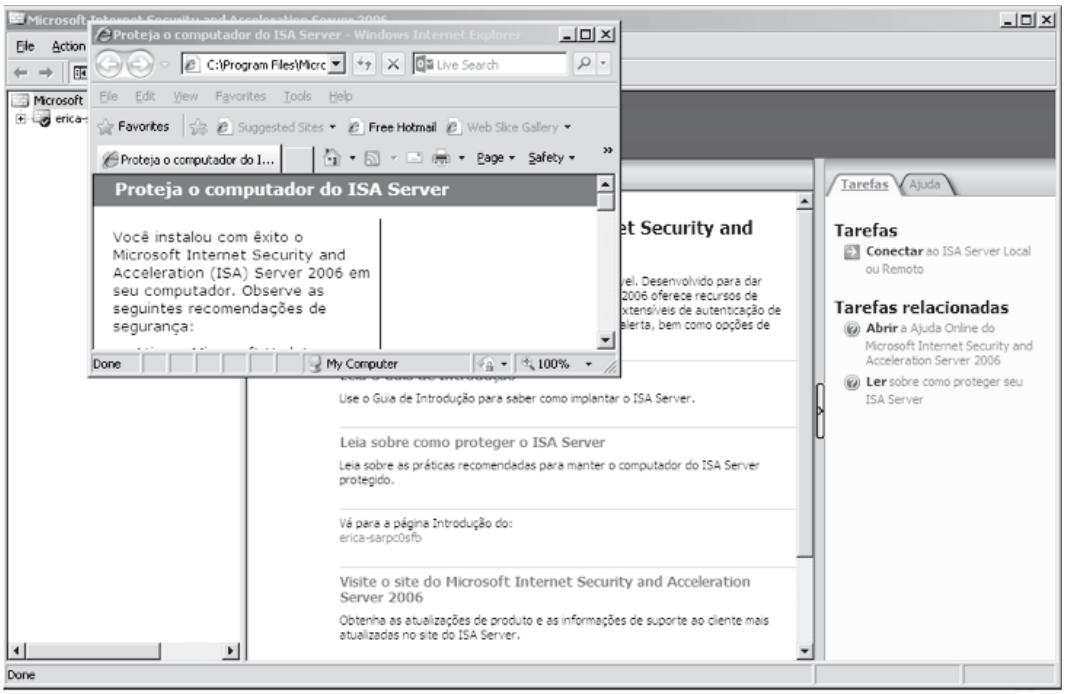


Figura 4.19 – Página inicial do ISA Server.

4.5 Monitoração

Para monitorar o status do ISA você deve clicar na Opção Monitorando logo após o servidor. Aí você terá dados do desempenho, dos alertas, das sessões, dos serviços, relatórios, conectividade e logs. Na Figura 4.20 é possível visualizar o painel de monitoração do ISA Server.

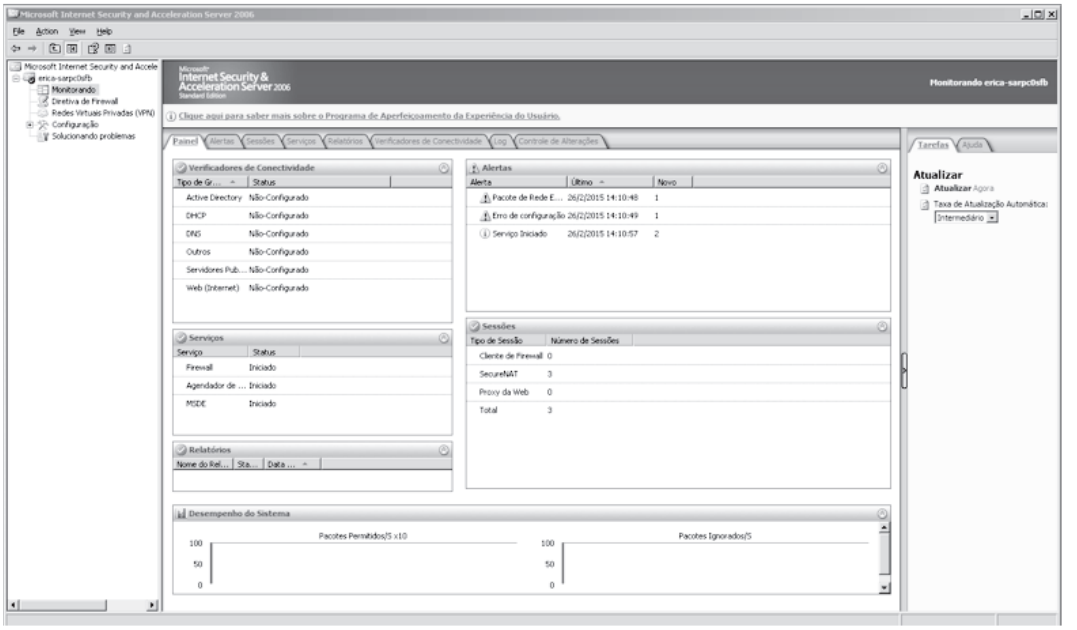


Figura 4.20 – Painel de monitoração do ISA Server.

4.6 Configuração

Na opção diretiva do firewall podemos observar as regras que foram configuradas. Observe que o ISA já vem com uma regra padrão de bloqueio de todo o tráfego, como podemos observar na Figura 4.21.

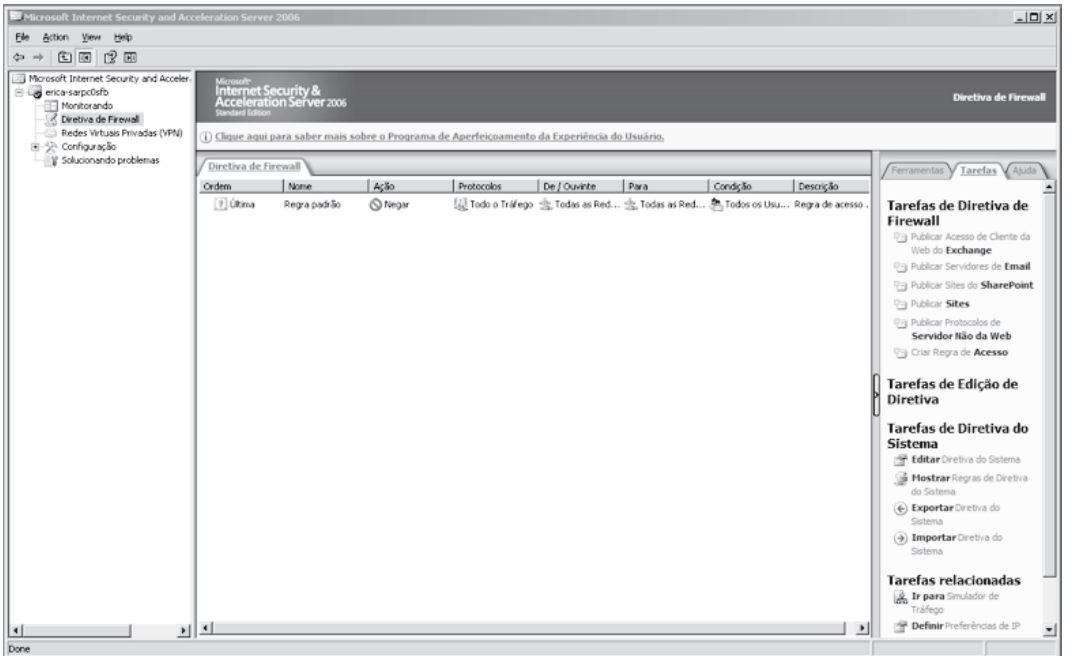


Figura 4.21 – Tela de políticas do firewall.

Na opção de Redes, podemos configurar as interfaces de Rede para criarmos uma rede Interna e outra Externa; na Figura 4.22 temos estas opções:

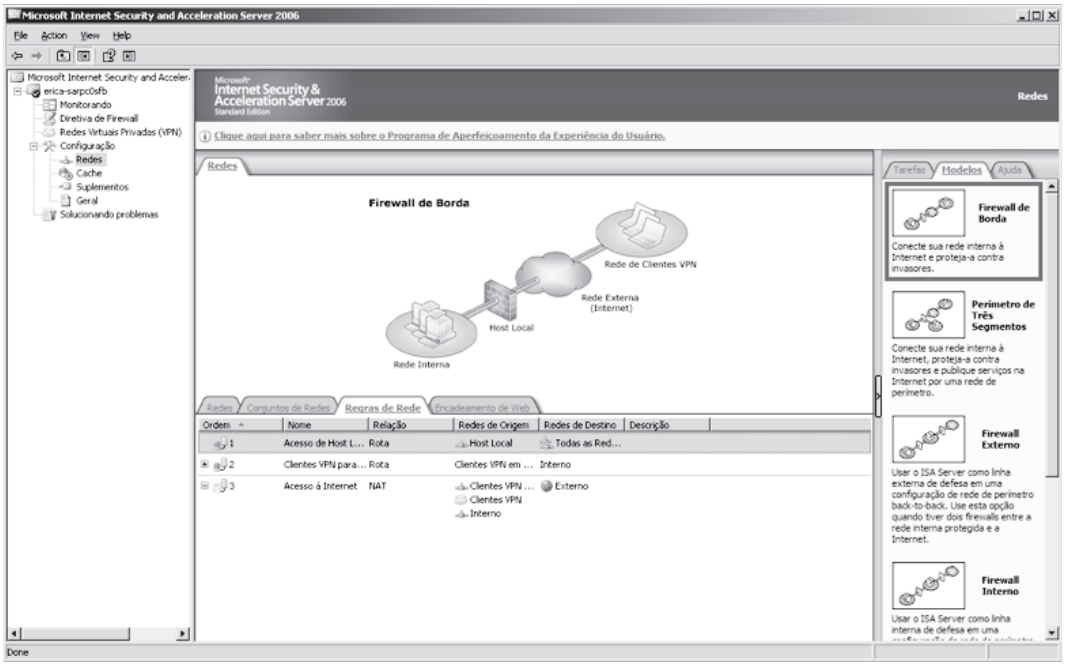


Figura 4.22 – Configurações de rede.

Na opção de Cache podemos observar as políticas de configuração do Cache no ISA Server.

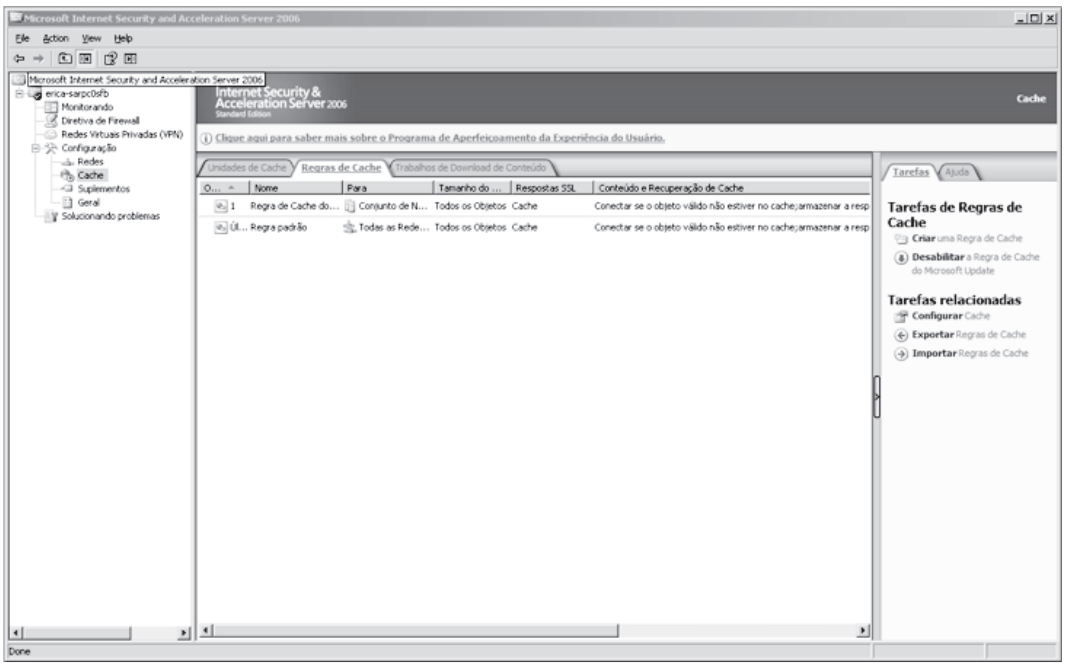


Figura 4.23 – Políticas de cache.

Na parte de suplementos podemos observar a parte de filtros de aplicativos, como vemos na Figura 4.24.

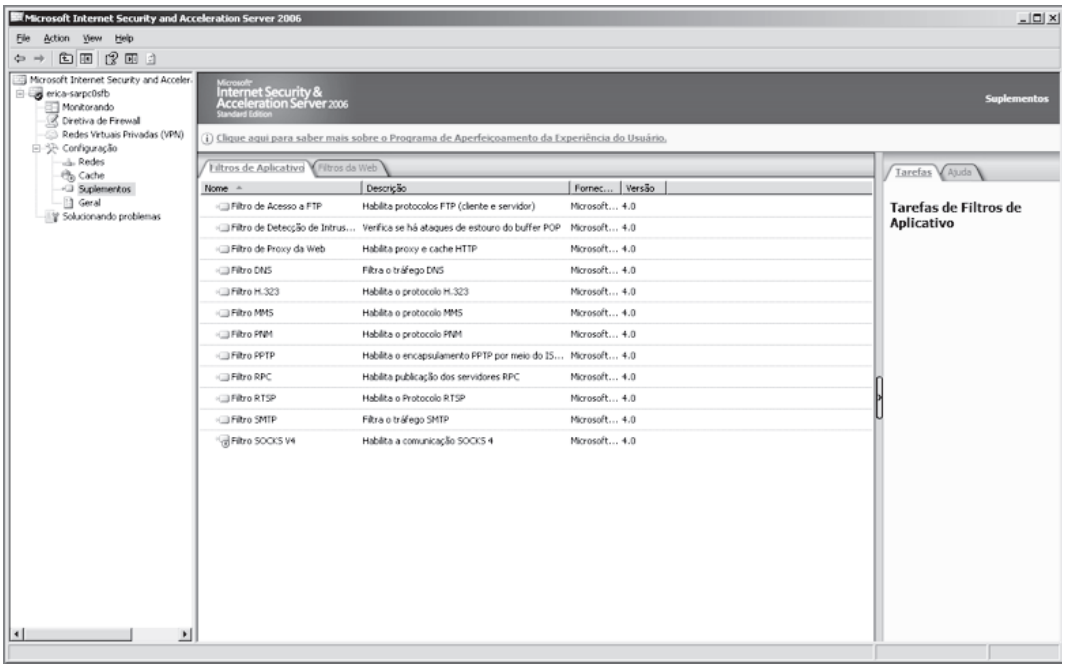


Figura 4.24 – Filtros de aplicativos.

E na Figura 4.25 podemos verificar os filtros de web.

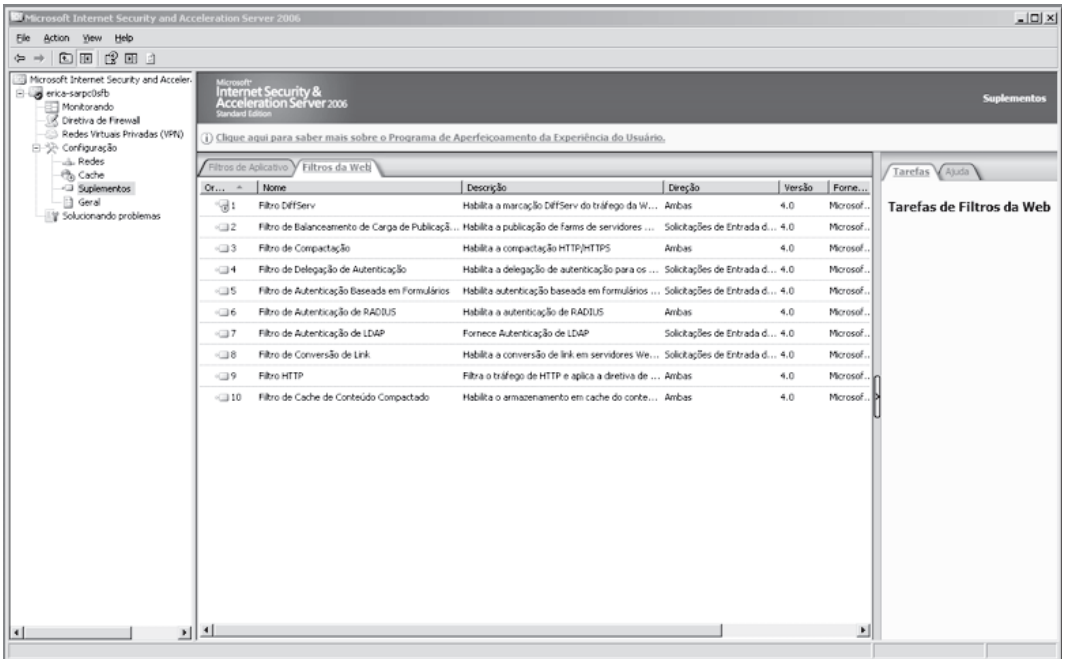


Figura 4.25 – Filtros de web.

Vamos recapitular?

O Microsoft ISA é um firewall do tipo proxy muito completo. Neste capítulo apresentamos os recursos, a arquitetura, o processo de instalação e visitamos as principais páginas de monitoração, de políticas, configuração de rede, cache e suplementos.

Agora é com você!

1) Como podemos classificar o Microsoft ISA Server dentro da arquitetura de firewall?
2) Qual a vantagem de possuir integração como diretório ativo?
3) Na instalação padrão do ISA normalmente consideramos quantas interfaces de rede?
4) Onde podemos encontrar as políticas de firewall?
5) Onde se encontram os logs do ISA Server?
6) Qual o protocolo de autenticação padrão do Active Directory que foi apresentado neste capítulo?

5

Introduzindo o Squid

Para começar

Este capítulo apresenta o funcionamento do Squid, um proxy poderoso baseado em software livre e muito utilizado. Abordaremos sua tecnologia e sua arquitetura, ensinaremos como instalá-lo e vamos finalizar com um exemplo de configuração.

5.1 O que é Squid?

Vamos começar definindo o que significa o termo "squid" em inglês. Segundo o dicionário Oxford, a palavra refere-se a: "um molusco com oito braços e dois tentáculos que nada rápido e tem a capacidade de mudar de cor". Ou seja, "squid", em português, é uma lula.

Provavelmente, o criador do termo quis fazer uma analogia entre os tentáculos e os braços do molusco com os protocolos suportados pelo Squid.

5.2 Squid, o proxy

Tecnicamente falando, o Squid é um firewall que usa a tecnologia de proxy. Ele faz proxy para os principais protocolos que utilizamos hoje na Internet. Além de ser um proxy, o Squid também pode fazer cache de páginas web.

Amplie seus conhecimentos

Você sabe como funciona um cache?

Basicamente, um cache armazena em seus discos as principais páginas que foram acessadas. A ideia é garantir que, quando houver um novo acesso, este ocorra diretamente do disco, e não seja baixada novamente a página da Internet. Esse processo tende a acelerar a velocidade de acesso às informações, uma vez que a página do cache é acessada mais rapidamente.

Para exemplificar, vamos dizer que o usuário João acessou a página <www.editoraerica.com.br>. Essa página, como não estava armazenada no cache, será baixada da Internet. João recebe a informação no seu browser e uma cópia fica armazenada no cache. Alguns minutos depois a usuária Maria, no mesmo computador, tenta também acessar o site da Editora Érica para buscar um livro. A página principal do site já está no cache, portanto, em vez de Maria receber a página principal da Internet, ela recebe diretamente do cache. O processo é simples e dá um bom resultado. Há mecanismos também para se atualizar o cache de tanto em tanto tempo, para não deixar desatualizadas as informações nele contidas.

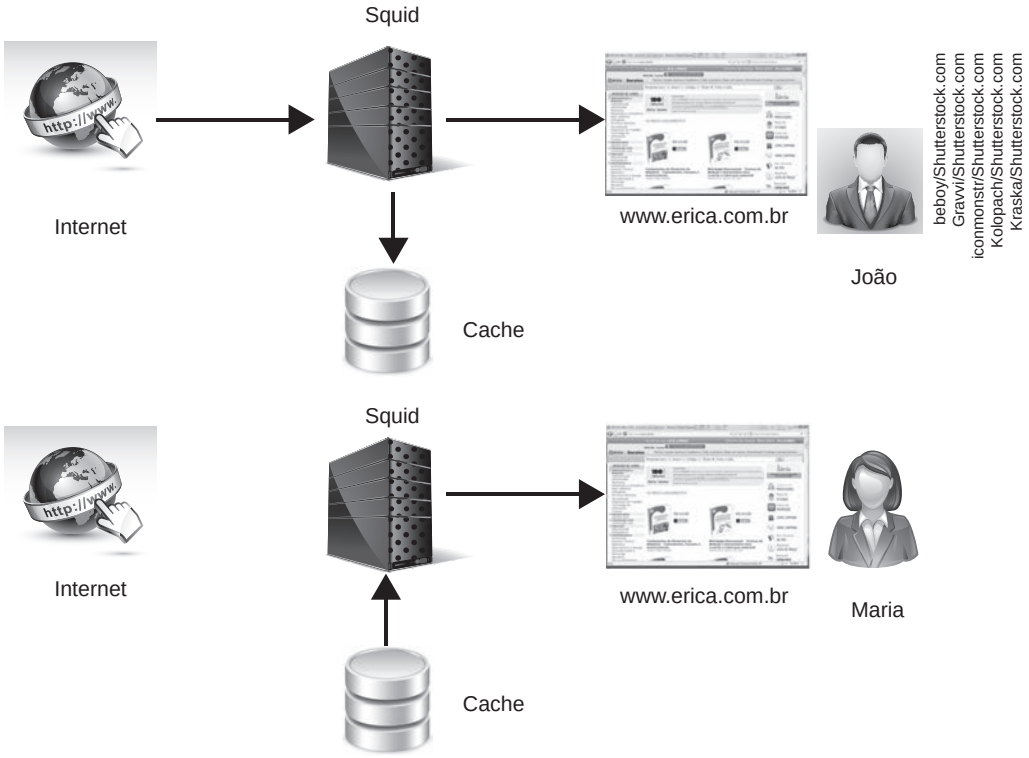


Figura 5.1 – Funcionamento do cache.

O proxy pode ser considerado um tecnologia de firewall que fica entre a rede interna e a rede externa. Desde o início, o objetivo do uso de proxies sempre foi a melhoria de performance no acesso à web, como fica claro no exemplo do cache. Porém, os proxies nos ajudam a garantir a navegação anônima dos usuários, uma vez que a conexão final ao servidor de destino é sempre do proxy com seu endereço IP.

Um dos recursos interessantes do proxy é a capacidade de trabalhar como filtro de conteúdo das conexões web, porque as conexões dos usuários sempre são estabelecidas junto ao proxy, que então faz a comunicação com a máquina final.

Algumas das vantagens de usarmos um proxy como o Squid:

» O Squid fica em um ponto central para controle de acesso e log.

» O proxy pode filtrar conteúdo malicioso se estiver, por exemplo, integrado a um antivírus.

» Capacidade de bloquear URLs.

» Faz a terminação das conexões dos clientes.

» Mascara os endereços locais da rede para a rede externa, que só enxerga o endereço do proxy.

» Os proxies podem fazer cache das requisições de DNS também.

» Vantagem de aumentar a capacidade do cache.

» Um proxy pode trabalhar em direção reversa, o que permite balancear carga.

Alguns problemas da implementação de proxies:

» Um proxy pode ser considerado um ponto único de falha.

» Os clientes devem estar preparados para trabalhar com o proxy, ou seja, deve haver uma configuração específica para isso.

» O proxy não protege o sistema operacional da máquina em que está instalado, uma vez que trabalha na camada de aplicação apenas.

O Squid, portanto, trabalhando como um proxy para as conexões web, consegue aumentar a velocidade fazendo o cache das páginas, como vimos na Figura 5.1. Na verdade, todos os usuários que estão configurados com o Squid como proxy estabelecem uma sessão ao Squid, e este, por sua vez, estabelece uma nova sessão à página de destino. O Squid, por arquitetura, limita-se a um pequeno grupo de protocolos com os quais pode trabalhar. São eles, basicamente: HTTP, HTTPS, SSL, TLS e FTP.

Por ser baseado em software livre, o Squid pode ser utilizado sem nenhum tipo de restrição. Ele foi criado originalmente para trabalhar com Sistemas Unix, porém, hoje, vem sendo utilizado em grande escala pelas principais distribuições Linux do mercado.

5.3 Onde nasceu o projeto do Squid?

O Squid nasceu de um projeto dos anos 1990, desenvolvido inicialmente pela Universidade do Colorado na cidade de Boulder, nos Estados Unidos. Porém, houve cooperação de outras universidades, como a Universidade da Califórnia em São Diego, e patrocínio da National Science Foundation. O nome do projeto original que gerou o Squid era “Harvest Project” e, na verdade, tratava-se de um projeto de tecnologia de cache, e não de firewall.

A primeira versão foi oficialmente lançada em julho de 1996 e, como virou software livre, ele vem sendo atualmente desenvolvido na comunidade Linux por voluntários. Mesmo sendo um software livre, o Squid é muito poderoso e vem sendo utilizado principalmente quando existe a necessidade de se fazer cache das páginas da Internet e controlar o acesso às aplicações web.

Como o proxy reescreve todo o pacote, ele trabalha na camada de aplicação, conseguindo assim fazer uma análise mais detalhada dos pacotes e das requisições. Como o usuário necessita estabelecer uma conexão com o proxy, faz-se necessária a configuração do proxy nas configurações de conexão do browser.

Apenas como exemplo: se a empresa possui um proxy trabalhando no endereço IP 192.168.1.100 e na porta 3128, esses dados precisam ser configurados. Além disso, o proxy pode ser configurado para autenticar as conexões, ou seja, apenas os usuários autenticados e autorizados podem acessar a Internet.

Os passos para fazer essa configuração utilizando o Mozilla Firefox são:

» 1.º passo: clique no ícone de configuração e, em seguida, escolha "Opções".

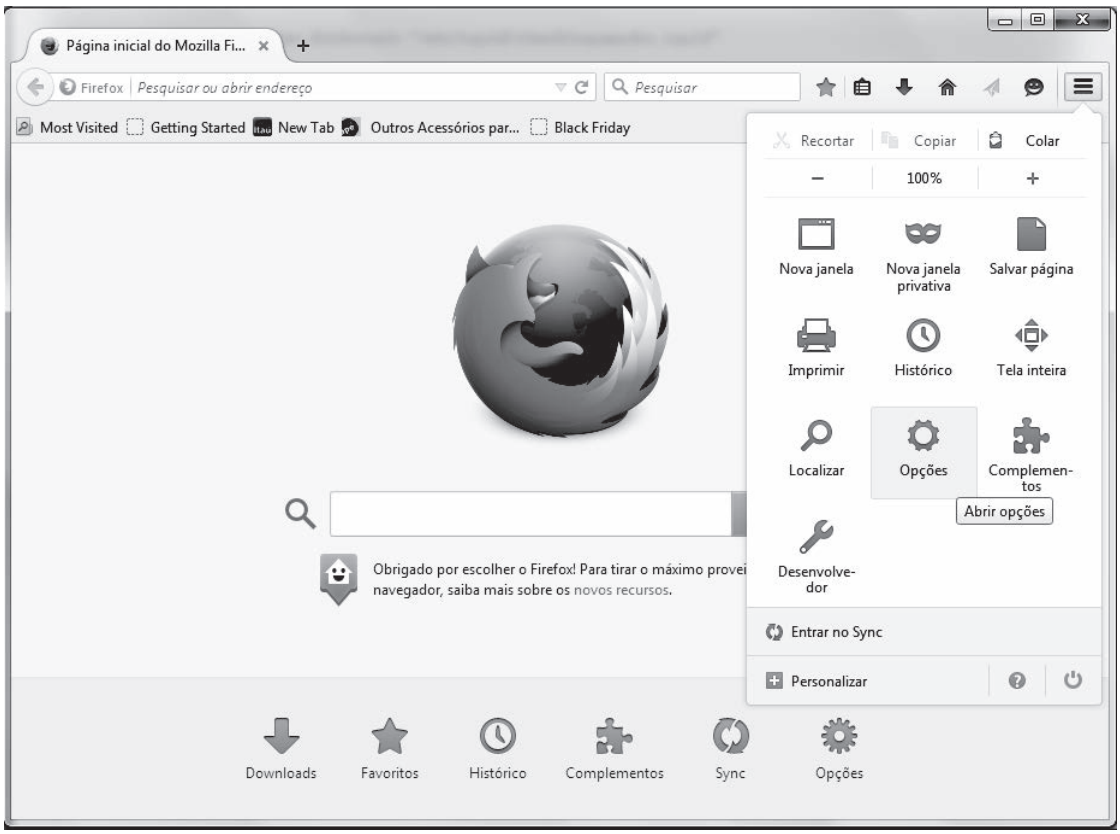


Figura 5.2 – Configuração de opções.

» 2.º passo: escolha a opção “Rede” no menu.

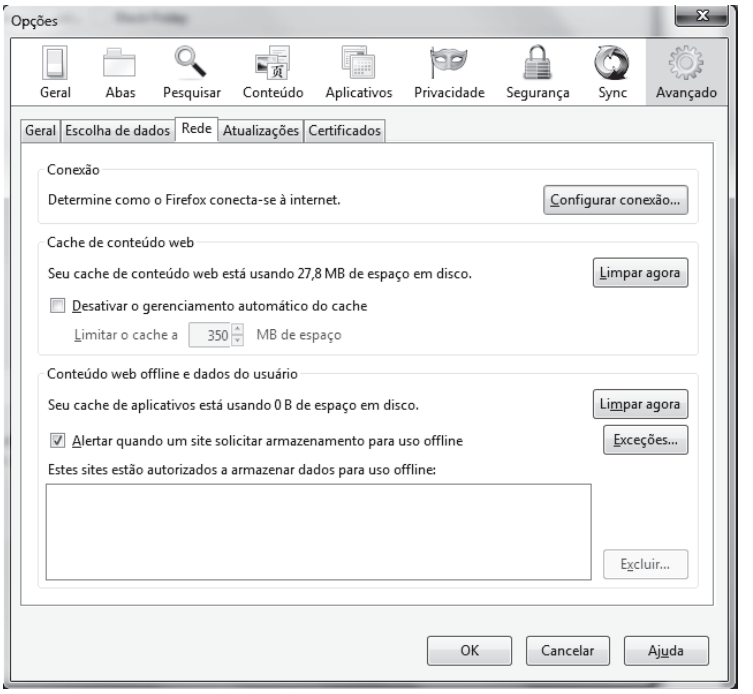


Figura 5.3 – Configuração de rede.

» 3.º passo: em seguida, clique na opção Configurar Conexão e configure o Acesso à Internet via Configuração Manual de Proxy, adicionando o IP do Squid, 192.168.1.100, e a porta 3128.

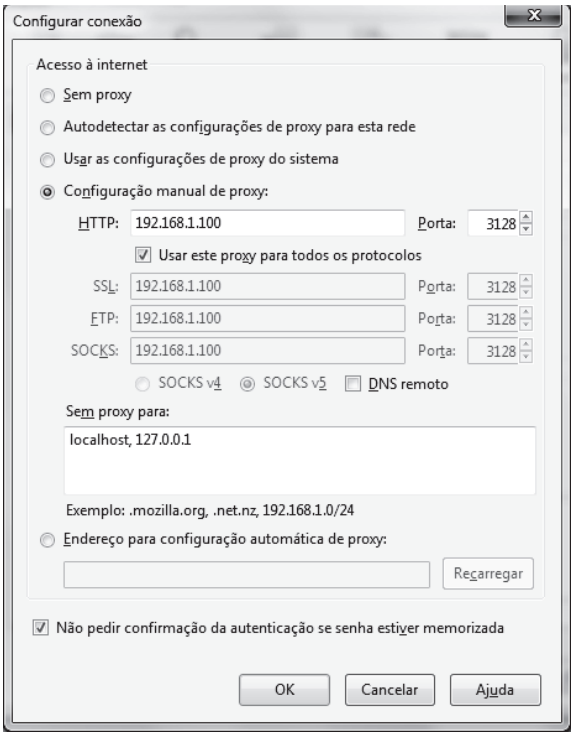


Figura 5.4 – Configuração dos endereços e porta do Squid.

5.4 O Squid como proxy transparente

O Squid pode também trabalhar no modo transparente. Nesse modo, não existe a necessidade de nenhuma configuração adicional nos clientes. Basicamente, o usuário acha que está fazendo a conexão diretamente ao servidor destino, porém, o proxy acaba sendo responsável por capturar e processar a solicitação.

Entre outras coisas, o proxy captura a requisição de DNS, e, para minimizar esse processo, é interessante configurarmos um servidor de DNS interno ao proxy. O proxy então captura essa sessão e faz a inspeção.

Um ponto importante: quando usamos proxy transparente é necessário que a máquina cliente conheça a rota para chegar até o servidor destino, o que pode representar uma vulnerabilidade caso o cliente esteja infectado (uma vez que ele pode tentar sair diretamente para a Internet). Quando o proxy não é transparente, não existe esse risco.

5.5 O Squid como proxy reverso

Um proxy reverso, diferentemente de um proxy tradicional, é utilizado para o tráfego de entrada, e não para o de saída. Normalmente, ele fica na frente dos servidores web tradicionais, e as conexões externas são então enviadas e roteadas a esse proxy, que normalmente é utilizado para balancear a carga entre servidores web com a mesma configuração e as aplicações. O proxy reverso, então, basicamente encaminha as solicitações externas a um conjunto de um ou mais servidores .

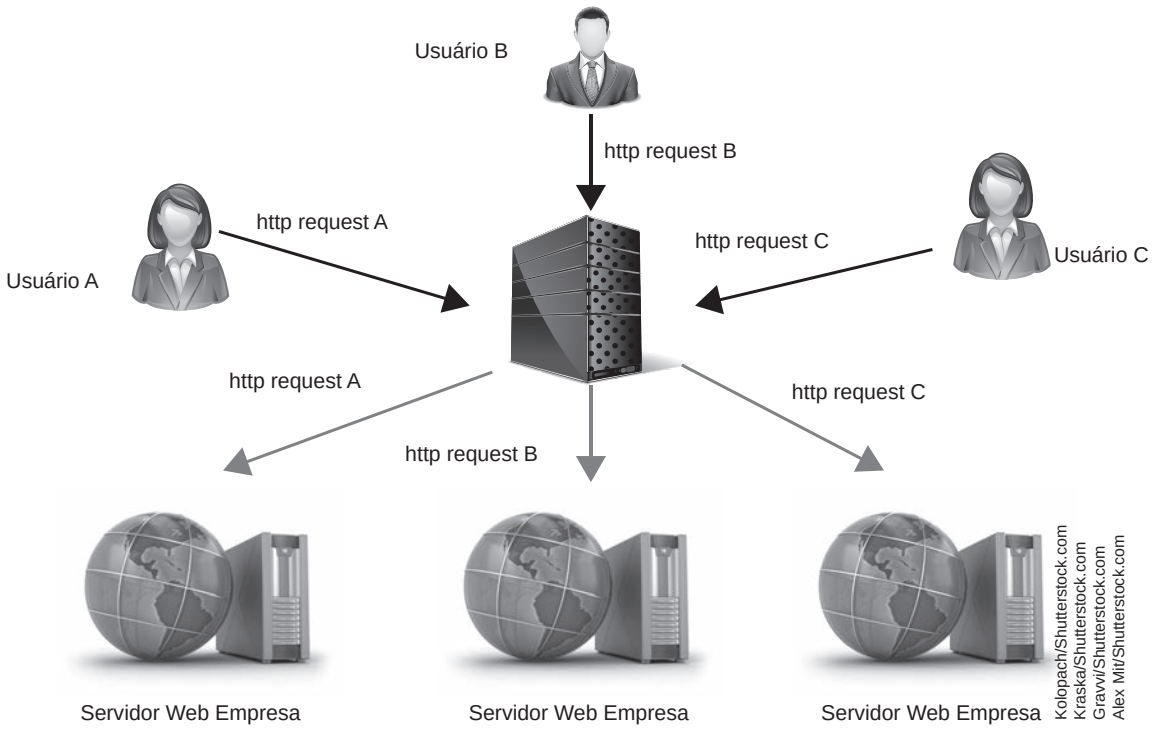


Figura 5.5 – Proxy reverse.

5.6 HTTP_X_FORWARD_FOR

Com esse recurso, o proxy armazena a informação do endereço IP do cliente que se conectou ao proxy no próprio pacote que o proxy vai gerar até o servidor de destino. Trata-se de um arranjo interessante, porque normalmente as conexões saem com o endereço IP do proxy. Sendo assim, se houver um ataque e usarmos alguma ferramenta de detecção, como um IPS (Intrusion Prevention System), essa informação pode servir para identificar o endereço real da máquina cliente que está conectada ao proxy.

Nada mais é do que um recurso que, quando habilitado, inclui essa informação no pacote reescrito ao destino.

5.7 Instalação do Squid

No CentOS é relativamente simples fazer a instalação do Squid.

```
# yum update
# yum install squid
```

Verifique o arquivo de configuração /etv/Squid/squid.conf

```
# service squid start
```

Instalação manual

A instalação manual é mais trabalhosa e envolve alguns passos adicionais.

» 1.º passo: primeiro, verifique a distribuição que voce está utilizando. O Squid pode ser instalado nas seguintes distribuições BSD:

CentOS.

Redhat.

Fedora.

Debian.

Gentoo.

» 2.º passo: vamos baixar os arquivos do Squid.

Para isso, recomendamos baixar o arquivo tar disponível no site: <http://www.squid-cache.org>.

Baixe sempre a última versão. Quando da publicação deste livro, a versão disponível no site era a 3.5.2.

Com o nome do arquivo squid-3.5.2.tar.gz

» 3.º passo: descompactar o arquivo.

```
# tar -vxf squid-3.5.2.tar.gz
```

» 4.º passo: vá ao diretório dos arquivos.

```
# cd squid-3.5.2
```

» 5.º passo: segundo o próprio site <www.squid-cache.org>, recomenda-se usar as seguintes opções no configure:

```
# ./configure -enable-underscores -prefix=/home/squid -enable-linux-netfilter
```

Significado:

Comando	Significado
`-enable-underscores`	Permite o uso de underscore nas URLs
`-enable-linux-netfilter`	Permite o uso de proxy transparente

» 6.º passo: vamos executar o comando make:

```
#make
```

» 7.º passo: por último, com o comando make install, o Squid será instalado na pasta /usr/local/squid

```
#make install
```

5.8 Configuração do Squid

A configuração e gerenciamento do Squid envolvem as seguintes etapas:

» Definição das interfaces de rede e tipo de proxy que será utilizado.

» Monitoramento dos logs.

» Definição das ACLs – Access Control List.

5.8.1 Definição das interfaces

Nessa etapa, definimos os endereços IP das interfaces e em quais portas queremos fazer proxy. Existem algumas portas que já estão definidas no arquivo de configuração, localizado em /etc/squid/squid.conf.

O arquivo de configuração default do Squid tem o seguinte conteúdo:

```
http_port 3128

refresh_pattern ^ftp:           1440    20%     10080
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

acl localnet src 10.0.0.0/8     # RFC 1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC 1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC 1918 possible internal network
acl localnet src fc00::/7       # RFC 4193 local private network range
```

```
acl localnet src fe80::/10      # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443          # https

acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http

acl CONNECT method CONNECT

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localnet
http_access allow localhost
http_access deny all
```

Podemos observar aí as portas default dos serviços. O serviço de http proxy vem configurado na porta default 3128.

Por exemplo, se desejarmos mudar a porta de acesso do Squid, devemos editar o arquivo /etc/squid/squid.conf. Vamos substituir a porta padrão pela nova porta, que, neste exemplo, será a porta 3180.

```
http_port 3180
```

Toda vez que for necessário reiniciar o serviço do Squid precisaremos executar os comandos a seguir:

`#service squid start` – Para iniciar o serviço do Squid

`#service squid stop` – Para interromper o serviço do Squid

`#service squid status` – Para verificar o status do serviço do Squid

5.8.1.1 Configuração dos parâmetros de cache

Se vamos usar o Squid como um cache, também é importante que os parâmetros para isso sejam customizados. A seguir, há um exemplo de customização do cache. Essas linhas devem estar no arquivo /etc/squid/squid.conf

```
Cache_mem 800 MB
Maximum_object_size_in_memory 32kb
Maximum_object_size 1024 MB
Minimum_object_size 0 Kb
Cache_swap_low 90
```

5.8.2 Gerenciamento dos logs

Os logs nos oferecem muita informação a respeito do funcionamento do Squid e de sua performance, e não apenas informações de acessos e erros de configuração. Existem vários arquivos que nos fornecem informações de logs. Os principais são CACHE_ACCESS_LOG, CACHE_LOG e CACHE_STORE_LOG.

```
CACHE_ACCESS_LOG
```

Nesse arquivo encontramos todas as informações de acessos dos clientes. Se ACLs não tiverem sido configuradas, todas as requisições dos clientes serão logadas neste arquivo, que pode ser acessado no seguinte diretório:

```
/home/squid/var/logs/access.log
```

Para acessar o conteúdo desse arquivo, simplesmente execute o comando:

```
# tail -f /home/squid/var/logs/access.log
CACHE_LOG
```

Nesse arquivo temos todas as informações de saúde e comportamento do cache. Nele, encontramos arquivos de configuração e informações do log acerca de erros de operação.

Quando tivermos algum problema com o Squid, este é o primeiro lugar que temos que checar para identificar o que pode ter ocorrido e encontrar a solução.

O arquivo encontra-se no seguinte diretório:

```
/home/squid/var/logs/cache.log
```

Para acessar o conteúdo do arquivo, simplesmente execute o comando:

```
# tail -f /home/squid/var/logs/cache.log
CACHE_STORE_LOG
```

Nesse arquivo são armazenados o log de transação e todos os objetos, além de informações a respeito de quando objetos foram apagados. Normalmente, a informação é usada apenas para a realização de debug.

O arquivo encontra-se no diretório:

```
/home/Squid/var/logs/store.log
```

Para acessar o conteúdo do arquivo, simplesmente execute o comando:

```
# tail -f /home/Squid/var/logs/store.log
```

5.8.3 Access control lists

Com as ACLs ("Access Control Lists") podemos limitar a capacidade dos usuários de navegarem na Internet. Normalmente, as informações que podemos utilizar para a criação de ACLs são:

- Endereço IP de origem / Endereço IP de destino.
- Domínio de origem / Domínio de destino.
- Expressão regular que dá match em um domínio.
- Palavras em uma URL específica.
- Palavras em um domínio de origem ou destino.
- Dados de dia e hora.
- Porta destino.
- Protocolo (FTP, HTTP e SSL).
- Método HTTP usado (HTTP Get ou HTTP Post).
- Tipo de browser utilizado.
- Usuário/senha.

O Squid faz um match das requisições web verificando os http_access sempre de cima para baixo. Quando uma regra é permitida ou negada, ele para a execução e não lê as regras que estão abaixo. Por isso, temos que tomar um cuidado danado para não criar conflitos de regras, isto é, incluir uma negação (deny) que bloqueie algo que seja permitido por outra regra.

A regra final do Squid é http_access deny all, que nega todo o tráfego.

5.9 Configurando o Squid para bloquear websites

Vamos dar os passos de configuração do Squid para filtragem dos seguintes websites:

- YouTube: www.youtube.com
- LinkedIn: www.linkedin.com
- Facebook: www.facebook.com
- Skype: www.skype.com

» 1.º passo: vamos criar o arquivo sitesbloqueados.squid

Executar o comando #cat /etc/squid/sitesbloqueados.squid

sites bloqueados

www.youtube.com

www.linkedin.com

www.facebook.com

www.skype.com

» 2.º passo: vamos editar o arquivo /etc/squid/squid.conf e criar uma nova ACL apontando para o arquivo sitesbloqueados.squid

```
acl bloquearsites dstdomain "/etc/squid/sitesbloqueados.squid"
```

» 3.º passo: criar uma linha com o http_access para bloquear o acesso

```
http_access deny bloquearsites
```

» 4.º passo: vamos reiniciar o serviço

```
Service squid restart
```

» 5.º passo: realizar testes nas máquinas da rede interna, tentando acessar os sites. As máquinas devem apresentar erro na tentativa de conexão.

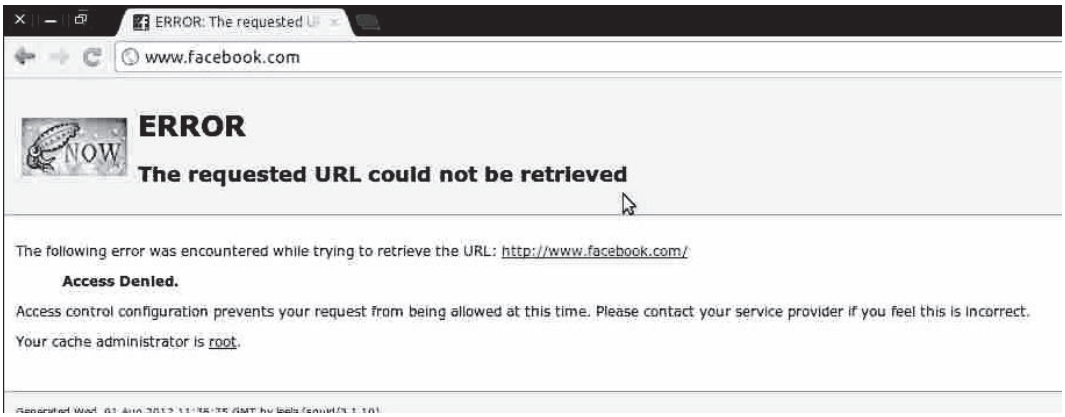


Figura 5.6 – Mensagem de erro ao acessar o Facebook.

» 6.º passo: verificar o arquivo de log às páginas bloqueadas

```
tail -f /var/log/squid/access.log
```

No arquivo você deverá encontrar uma linha:

```
TCP/DENIED/407   GET   http://www.facebook.com/ - NONE / -text/html
```

5.10 Configurando o Squid para bloquear determinadas palavras na URL

A ideia dessa configuração é bloquear URLs que possuam uma das palavras na lista.

» 1.º passo: criar um arquivo bloquearpalavras.

```
Cat /etc/squid/bloquearpalavras
```

bloquear palavras

Emprego

XXX

Porn

» 2.º passo: vamos abrir o arquivo /etc/squid/squid.conf e criar uma ACL bloquear_palavras.

```
Acl bloquear_palavras url_regex -i "/etc/squid/bloquearpalavras.squid"
```

» 3.º passo: vamos criar a regra http_access para bloquear palavras.

```
http_access deny bloquear_palavras
```

5.11 Restringindo o acesso de um IP específico

A ideia é bloquear o acesso de um determinado endereço IP.

» 1.º passo: criar a lista com o endereço IP que desejamos bloquear no arquivo bloquearIP.squid.

```
# bloquear IP
10.10.3.20
```

» 2.º passo: abrir o arquivo de configuração /etc/squid/squid.conf e criar uma nova ACL "bloquear_IP".

```
acl bloquear_IP src "/etc/squid/bloquearIP.squid"
```

» 3.º passo: criar o http_access para o bloqueio.

```
http_access deny bloquear_IP
```

5.12 Criando exceções para que determinadas máquinas acessem sem restrição

O objetivo aqui é permitir que um grupo de máquinas realize o acesso sem sofrer restrição pelo Squid, ou seja, estamos criando uma exceção às regras.

» 1.º passo: criar o arquivo com os endereços IP que serão permitidos.

```
cat /etc/squid/IPpermitido.squid
# IPs permitidos
10.10.3.100
10.10.3.101
10.10.3.102
10.10.3.103
10.10.3.104
```

» 2.º passo: criar a regra de ACL para permitir os IPs

```
# acl permitir_ip src "/etc/squid/Ippermitido.squid"
```

» 3.º passo: nas regras que foram criadas, como a do exemplo 5.9, precisamos incluir uma exclamação "!" para incluir a exceção no http_access.

```
# http_access deny bloquearsites  ! permitir_ip
```

Vamos recapitular?

Neste capítulo aprendemos o que é o Squid e o seu funcionamento como proxy. Pudemos entender conceitos importantes, como os de proxy reverso e proxy transparente, e os processos de definição de interfaces, criação de regras de acesso e monitoramento da ferramenta. Concluímos com exemplos práticos de configurações.

Agora é com você!

1) Qual era o objetivo do projeto original do Squid?
2) Qual a principal vantagem do uso do cache?
3) Em termos da proteção do usuário final (cliente), qual é a vantagem oferecida pelo Squid?
4) Apresente pelo menos duas vantagens de trabalharmos com o Squid.
5) Qual a desvantagem ou o risco de usarmos o proxy?
6) Qual a porta default que vem configurada no Squid?
7) Como se chama o arquivo que armazena o log dos acessos? Onde ele se localiza?
8) Como funciona o proxy reverso? Qual a sua principal utilização?
9) O que é o proxy transparente? O que muda quando utilizamos essa configuração?
10) Quando criamos uma regra de http_access, o que representa o uso de um sinal de exclamação "!"?

6

Introduzindo o IP Tables

Para começar

Neste capítulo vamos ver em detalhes como funciona o IP Tables, um poderoso filtro de pacotes que já acompanha a maior parte dos sistemas e distribuições Linux do mercado. Vamos estudar conceitos, arquitetura, o NAT em detalhes e os principais comandos e opções de configuração.

6.1 IP Tables

O IP Tables nasceu do projeto open source, ou seja, de software de código aberto, conhecido como NetFilter. Esse pacote começou a ser disponibilizado nas distribuições 2.4 e 2.6 do Kernel do Linux. O IP Tables é o pedaço do NetFilter que nos permite manipular pacotes.

Por ser baseado em software livre, já vem disponibilizado em distribuições como Redhat, Cent OS, Ubuntu e Fedora.

Amplie seus conhecimentos

Você sabe como nasceu o Linux?

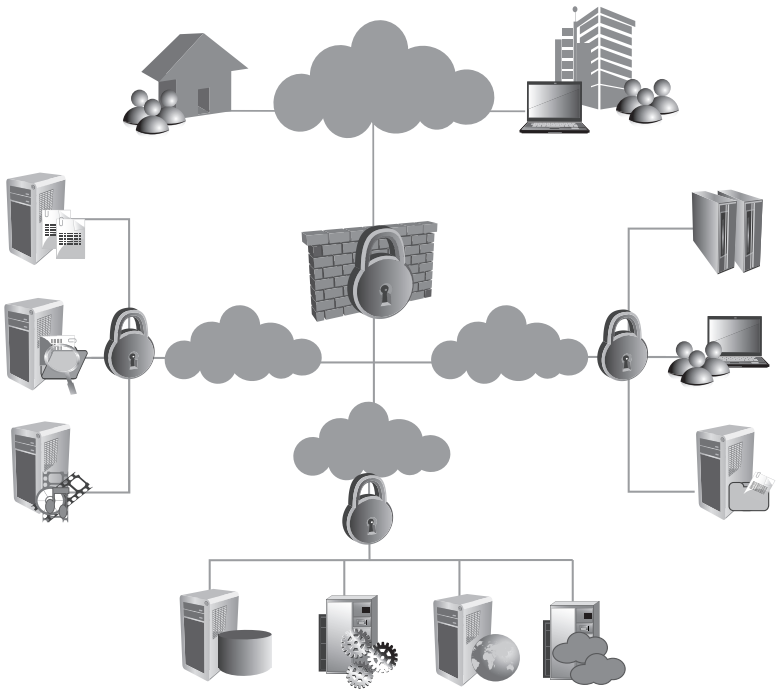
O Linux nasceu de um projeto criado em 1991 por Linus Benedict Torvalds com o objetivo de ser um sistema operacional livre e de código aberto. Embora a base do Kernel do Linux seja muito parecida com o Unix, que é um sistema proprietário, nunca se conseguiu comprovar que houve cópia ou engenharia reversa do Unix.

Hoje, o Linux e suas distribuições, que são adaptações do Linux original, são ferramentas e soluções de segurança muito utilizadas. Um conjunto muito grande de empresas utiliza firewalls baseados em tecnologia Linux.

claudionegri79/Shutterstock.com

Figura 6.1 – Linux.

A ideia do uso do IP Tables é analisar o tráfego que chega por suas interfaces e tomar decisões de permitir, bloquear e monitorar esse tráfego. Normalmente, a máquina em que o IP Tables é executado está posicionada no perímetro da rede. Seu objetivo, portanto, é filtrar o tráfego, permitindo o tráfego legítimo, que é autorizado, e bloqueando o tráfego não permitido.



TechnoVectors/Shutterstock.com

Figura 6.2 – IP Tables protegendo o perímetro.

As decisões que o IP Tables toma são baseadas em um conjunto de regras, que é conhecido como política de segurança do firewall. Há uma série de critérios para a definição dessas políticas, e um detalhe muito importante é a ordem com que essas políticas devem ser aplicadas.

A política de segurança é algo muito específico. Cada empresa ou organização possui necessidades próprias de segurança, cada uma delas precisa controlar o acesso de uma maneira diferente. Por exemplo, uma empresa A deseja disponibilizar o acesso a seu servidor FTP pela Internet. Para isso, é necessário criar um filtro que mantenha e administre a permissão desse acesso. Por outro lado, a empresa B deseja limitar o acesso do seu FTP apenas às máquinas internas da rede, bloqueando-se assim eventuais tentativas de acesso.

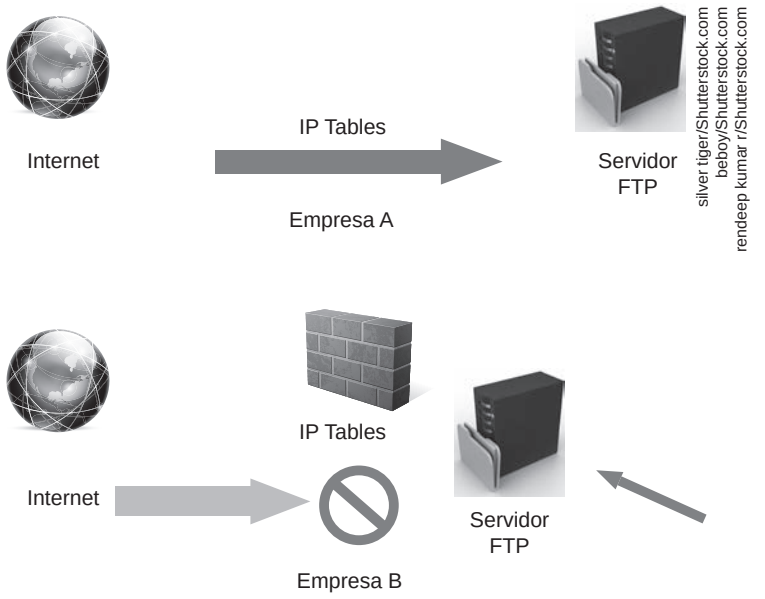


Figura 6.3 – Acesso ao FTP.

Cada empresa tem seus cenários e suas necessidades de segurança. As regras do IP Tables normalmente são executadas na sequência, ou seja, o tráfego é analisado, toda vez que chega um pacote, da primeira regra em diante. A regra que bater com os critérios será executada e o pacote será, desse modo, permitido ou bloqueado. É um fluxo de análise.

As regras são baseadas em sua grande maioria no endereçamento IP e na porta da aplicação. Porém, o IP Tables consegue também implementar filtros mais avançados baseados no endereçamento IP, nos flags do pacote TCP (informação da camada de transporte), no código do protocolo que está sendo utilizado, na URL (se for tráfego web) e podem ser criadas regras utilizando até informações de enlace do modelo OSI, como o MAC Address (Endereço MAC da estação).

Uma das coisas que mais impressiona no IP Tables é a sua velocidade e a sua robustez. Ele muitas vezes apresenta um desempenho muito superior ao de um firewall proprietário de mercado. Muito disse se deve ao fato de o IP Tables ser um pacote do Linux que é executado no Kernel do sistema operacional.

O IP Tables pode inclusive filtrar pacotes malformados, impedindo assim que um ataque ocorra. Ademais, um dos recursos mais interessantes do IP Tables é o NAT (Network Address Translation).

6.2 NAT (Network Address Translation) – Tradução Automática de Endereços

O NAT, ou Network Address Translation, nasceu como uma maneira de resolver e minimizar o problema do esgotamento de endereços IP versão 4. Já nos anos 90 havia uma previsão de que o endereçamento IP iria se esgotar rapidamente, e a solução definitiva seria o projeto do IP versão 6. Porém, ele só foi lançado em 1999, e, enquanto isso, o NAT foi implementado como uma solução de contorno.

Antes do NAT, cada empresa precisava ter um endereço válido na Internet para permitir o acesso à rede. Grandes companhias, como AT&T, Microsoft, Cisco, IBM e HP, obtiveram blocos inteiros de endereços IP válidos para uso interno.

Esse modelo, como já comentamos, estava a caminho da exaustão. Para solucionar o problema, desenvolveu-se o NAT, uma solução que traduz endereços de IP válidos em endereços internos privados que não são válidos na Internet.

A RFC 1918 definiu um conjunto de endereçamentos IP privados na Internet. São eles:

» 10.0.0.0 – 10.255.255.255 – Endereçamento Classe A privado – 1 classe.

» 172.16.0.0 – 172.31.255.255 – Endereçamento Classe B privado – 16 classes.

» 192.168.0.0 – 192.168.255.255 – Endereçamento Classe C privado – 256 classes.

O NAT cria uma tabela que traduz endereços válidos na Internet em endereços privados Inválidos utilizados na rede interna da empresa.

O NAT pode ser estático, dinâmico ou utilizar recursos de PAT (tradução automática de portas).

6.2.1 NAT estático

No NAT estático existe um conjunto de endereços IP válidos (públicos) que é traduzido para um conjunto de endereços IP internos privados. Esse cenário é utilizado para mapear servidores da empresa que necessitem de acesso pela Internet e, portanto, um endereço fixo.

6.2.2 NAT dinâmico

Ocorre quando o NAT é realizado a partir de um número limitado de endereços públicos. Os endereços privados da empresa são mapeados dinamicamente nesses endereços, e temos então a limitação de acessos pela quantidade de endereços IP.

Nesse caso, quando um usuário acessa um endereço na Internet, ele (o usuário) é dinamicamente mapeado a um desses endereços na Internet. Essa estratégica fazia com que as empresas comprassem apenas endereços necessários à demanda de acessos simultâneos à Internet.

6.2.3 PAT ("Port Address Translation")

O PAT, ou Port Address Translation (tradução de portas), é o método mais inteligente e mais utilizado, especialmente devido à grande limitação que temos hoje de endereços IP versão 4.

Essa técnica permite que vários computadores compartilhem um único endereço IP para sair para a Internet. Isso só é possível porque o PAT mantém uma tabela da conexão, e troca, além do endereço de origem da conexão pelo público, também a porta.

» Exemplo do funcionamento: um usuário interno no endereço 192.168.10.3 (privado) deseja estabelecer uma conexão web (porta 80) com o servidor localizado no endereço da Internet 200.204.0.10.

Sabendo-se que o endereço privado da empresa é 200.215.0.25, como deve funcionar esse processo?

» 1.º passo: o usuário abre a sessão criando um pacote IP com os seguintes campos:

Endereço IP Origem	Porta Origem	Endereço IP Destino	Porta Destino
192.168.10.3	4023 (aleatória, definida pelo sistema operacional)	200.204.0.10	80

» 2.º passo: em decorrência do roteamento, o pacote será direcionado pela rota default (nesse caso, o endereço IP da interface de rede interna – privada – do IP Tables).

» 3.º passo: o IP Tables faz algumas alterações no pacote, conforme a tabela abaixo.

Pacote original (interface interna)

Endereço IP Origem	Porta Origem	Endereço IP Destino	Porta Destino
192.168.10.3	4023	200.204.0.10	80

Pacote modificado (interface externa)

Endereço IP Origem	Porta Origem	Endereço IP Destino	Porta Destino
200.215.0.25	2023	200.204.0.10	80

O pacote a ser enviado para a Internet foi modificado considerando-se o IP de origem como o endereço público da empresa. Por quê?

Por um simples motivo: se o pacote saísse com o endereço privado, ele nunca voltaria, portanto, é necessário que saia com o endereço público da empresa.

O PAT trabalha de uma maneira em que a porta de origem é utilizada para identificar a conexão. Sendo assim, para evitar repetições, o PAT sempre troca a porta de origem.

» 4.º passo: vamos ver como fica o pacote de volta do servidor acessado.

Pacote original (interface externa)

Endereço IP Origem	Porta Origem	Endereço IP Destino	Porta Destino
200.204.0.10	80	200.215.0.25	2023

Pacote modificado (interface interna)

Endereço IP Origem	Porta Origem	Endereço IP Destino	Porta Destino
200.204.0.10	80	192.168.10.3	4023

Observe que os identificadores da conexão (para fazer a tradução) são o endereço IP (200.204.0.10) e a porta alocada (2023).

6.3 Como funciona o IP Tables na estrutura do Linux?

O IP Tables trabalha em conjunto com o Kernel do Linux e as funções de acesso à rede. Os principais módulos que são ativados no Kernel são:

» NF_IP_PRE_ROUTING: é a função que decide como o pacote será roteado.

» NF_IP_FORWARD: é a função que deve ser ativada caso o pacote precise ser enviado a outra interface de rede.

» NF_IP_LOCAL_OUT: é a função que deve ser ativada caso o pacote necessite ser enviado a outra máquina.

» NF_IP_POST_ROUTING: é a última função a ser ativada quando o pacote deixa a máquina do IP Tables.

O IP Tables trabalha em conjunto com essas três chamadas do sistema operacional. Ele possui três tabelas com as informações necessárias para tomar as decisões de encaminhamento: tabela de filtragem, NAT e Mangle.

6.3.1 Tabela de filtragem

Essa tabela inclui as regras de firewall que serão executadas para cada pacote que chega ao IP Tables. Um ponto muito importante é a ordem das regras na tabela, pois a execução sempre começa pelas regras mais prioritárias, que, portanto, devem ser colocadas mais acima.

6.3.2 Tabela NAT

Essa tabela realiza as funções de NAT conforme a técnica observada neste capítulo. Todas as tabelas de tradução ficam armazenadas nessa tabela.

6.3.3 Tabela Mangle

Essa tabela é responsável pelas alterações nos pacotes. Entre essas alterações inclui-se a mudança em alguns bits do cabeçalho TCP/IP, como o bit ToS.

6.4 Regras de firewall no IP Tables

De acordo com essas regras, é possível permitir ou negar determinado tipo de tráfego. Nas regras de firewall, podemos usar como parâmetros informações importantes, como endereçamento IP, portas e protocolos.

O IP Tables tem uma interface de linha de comandos, ou seja, para adicionarmos os comandos, basta inserirmos a linha em um terminal do Linux. Outro ponto interessante é que ele oferece o recurso de se trabalhar como um firewall stateful inspection, como vimos no Capítulo 2.

Para que possamos fazer a configuração do equipamento, é importante entender o conceito de Chain. O termo passa a ideia de uma "cadeia", ou seja, refere-se a como os pacotes encadeados serão tratados. Existe uma cadeia de entrada ("input chain") quando o tráfego entra sem ser tratado ou modificado, existe uma cadeia de encaminhamento ("forward chain") quando esse tráfego é encaminhado a outra máquina, e existe uma cadeia de saída ("output chain") quando o tráfego já foi tratado pelas regras do firewall.

Existem ainda duas cadeias importantes utilizadas no NAT dos pacotes: o PRE_ROUTING CHAIN são pacotes NAT em que o destino precisa mudar e o POST_ROUTING CHAIN são pacotes NAT em que a origem precisa mudar.

Os seguintes parâmetros podem ser utilizados para criarmos as regras com o IP Tables:

» IP ADDRESS (Endereço IP): tanto origem como destino, e as regras podem ser escritas para um endereço IP, uma rede/sub-rede ou uma faixa de endereços IP.

» PORTS (Portas): nessa informação temos a porta de origem/destino, e podemos também definir uma faixa de portas ou um conjunto de portas.

» PROTOCOLO: temos aqui a regra de qual protocolo será utilizado – pode haver referência aos protocolos TCP, UDP, ICMP, ou seja, protocolos de camada 3 e 4 do Modelo OSI.

» INTERFACE: aqui temos a interface de entrada e a interface de saída que serão aplicadas.

» TTL ("time to live"): é o campo existente nos pacotes de tempo de vida.

» TOS ("type of service"): é o campo de tipo de serviço.

» LENGTH: é o campo que define o tamanho do pacote.

» MAC DE ORIGEM: é o campo que define o endereço MAC de origem.

» SYN FLAG: é o flag da conexão TCP/IP.

» ICMP TYPE: é o código do pacote ICMP.

Tabela 6.1 – Principais comandos do IP Tables

Comando	Funcionamento
ACCEPT	Quando ocorre o ACCEPT o pacote é aceito, permitindo-se a conclusão do seu processamento.
DROP	O pacote é bloqueado e nenhum processamento adicional é necessário.
LOG	Quando usamos esse comando, um pacote de SYSLOG é criado e enviado ao servidor correspondente. Não é possível logar e bloquear ao mesmo tempo. Primeiro, precisamos logar e depois bloquear; assim sendo, são necessárias uma regra para logar e uma segunda para bloquear.
REJECT	Funciona como o DROP, mas envia um pacote de TCP RESET à origem informando que o pacote foi bloqueado.
DNAT	Usado para configurar regras de NAT dinâmico, reescrevendo o destino final do pacote.
SNAT	Usado na tradução e reescrita do endereço de origem do pacote.
MASQUERADE	No NAT, quando enviamos um pacote, o novo endereço de origem normalmente é o endereço da interface pública do IP Tables. O MASQUERADE é usado quando, por algum motivo, desejamos mascarar esse endereço de origem.

Na Tabela 6.2 podemos observar as principais opções no comando.

Tabela 6.2 – Principais opções do IP Tables

Opção	Comando	Significado
-A	Append	Adiciona uma ou mais regras no final da cadeia (chain).
-D	Delete	Apaga uma ou mais regras.
-R	Replace	Modifica uma das regras.
-I	Insert	Insere uma ou mais regras.
-L	List	Lista todas as regras de uma cadeia.
-F	Flush	Apaga toda uma cadeia.
-Z	Zero	Zera os contadores de bytes de determinada cadeia.
-N	New	Cria nova cadeia.
-X	Extract	Deleta uma cadeia.
-P	Policy	Define uma política.
-E	Rename	Renomeia uma cadeia.

Na Tabela 6.3 são apresentados alguns parâmetros adicionais.

Tabela 6.3 – Parâmetros adicionais utilizados no IP Tables

Parâmetro	Significado
-4	Denota o IP versão 4
-6	Denota o IP versão 6
-p	Define o protocolo TCP/UDP/ICMP/ESP AH (IPSEC)
-s	Define a origem (“source”)
-d	Define o destino (“destination”)
-m	Especifica o que faz disparar a regra
-j	Pula para uma determinada regra
-g	Vai para uma cadeia específica
-i	Nome da interface de entrada
-o	Nome da interface de saída
-f	Fragmento
-c	Contadores

6.5 Como instalar o IP Tables?

Inicialmente, recomendamos instalar uma máquina virtual ou uma distribuição de Linux. Apenas como sugestão, neste livro vamos trabalhar com o CentOS. Para baixar a distribuição e instalá-la, sugerimos ao leitor o site: <http://www.centos.org/download/>.

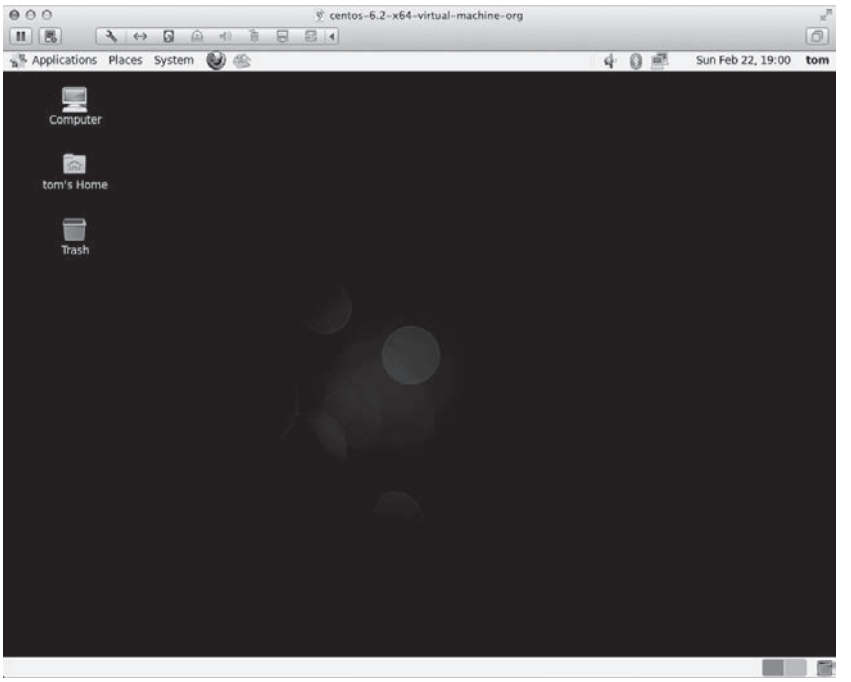


Figura 6.4 – Tela Inicial do CentOS.

Estamos usando o IP Tables que já vem instalado na maioria das distribuições do Linux. A nossa versão do CentOS é a 6.4. Para verificar se o IP Tables está instalado, simplesmente abra um terminal e execute o comando

```
# yum info iptables
```

Podemos ver na Figura 6.5 que o pacote já veio instalado na distribuição.

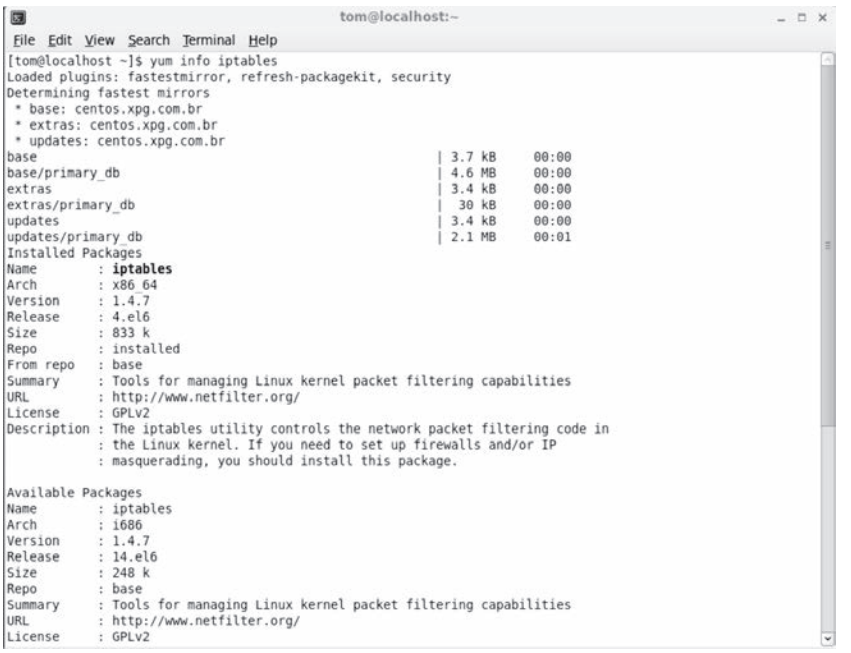


Figura 6.5 – Execução do comando yum info iptables.

Como já foi dito, quase todas as distribuições já vêm atualmente com o pacote do IP Tables instalado. Caso você esteja trabalhando com uma distribuição muito antiga, recomendamos usar o comando wget.

```
tom@localhost:~
File  Edit  View  Search  Terminal  Help
[tom@localhost ~]$ wget http://www.netfilter.org/projects/iptables/files/iptables-1.4.21.tar.bz2
```

Figura 6.6 – Comando wget para baixar o IP Tables.

Após a execução você verá que o arquivo será baixado, como observamos na Figura 6.7.

```
tom@localhost:~
File  Edit  View  Search  Terminal  Help
[tom@localhost ~]$ wget http://www.netfilter.org/projects/iptables/files/iptables-1.4.21.tar.bz2
--2015-02-22 19:33:06--  http://www.netfilter.org/projects/iptables/files/iptables-1.4.21.tar.bz2
Resolving www.netfilter.org... 150.214.142.167
Connecting to www.netfilter.org|150.214.142.167|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 547439 (535K) [application/x-bzip2]
Saving to: “iptables-1.4.21.tar.bz2.2”

100%[=============================================================>] 547,439     8.50K/s   in 36s

2015-02-22 19:33:42 (14.9 KB/s) - “iptables-1.4.21.tar.bz2.2” saved [547439/547439]

[tom@localhost ~]$
```

Figura 6.7 – Download do pacote do IP Tables.

O próximo passo é descompactar o arquivo, como na Figura 6.8.

```
tom@localhost:~
File  Edit  View  Search  Terminal  Help
[tom@localhost ~]$ bunzip2 iptables-1.4.21.tar.bz2
[tom@localhost ~]$ tar -xvf iptables-1.4.21.tar
```

Figura 6.8 – Descompactando o arquivo.

Em seguida, o usuário deverá executar os comandos:

» Configure.

» Make.

» Make install.

6.6 Exemplo prático

A empresa Suportek tem um acesso dedicado à Internet cujo endereço IP público é 173.73.73.73. A empresa deseja liberar o acesso apenas para os seguintes serviços:

Servidor de Correios SMTP – porta TCP 25 – IP interno 10.10.10.1

Servidor Web – porta TCP 80 – IP interno 10.10.10.2

Os usuários da rede interna deverão ter acesso apenas à web (porta 80), porém com algumas políticas de restrição a Facebook, YouTube e aplicações de P2P (Peer to Peer), como o Kazaa e o ARES.

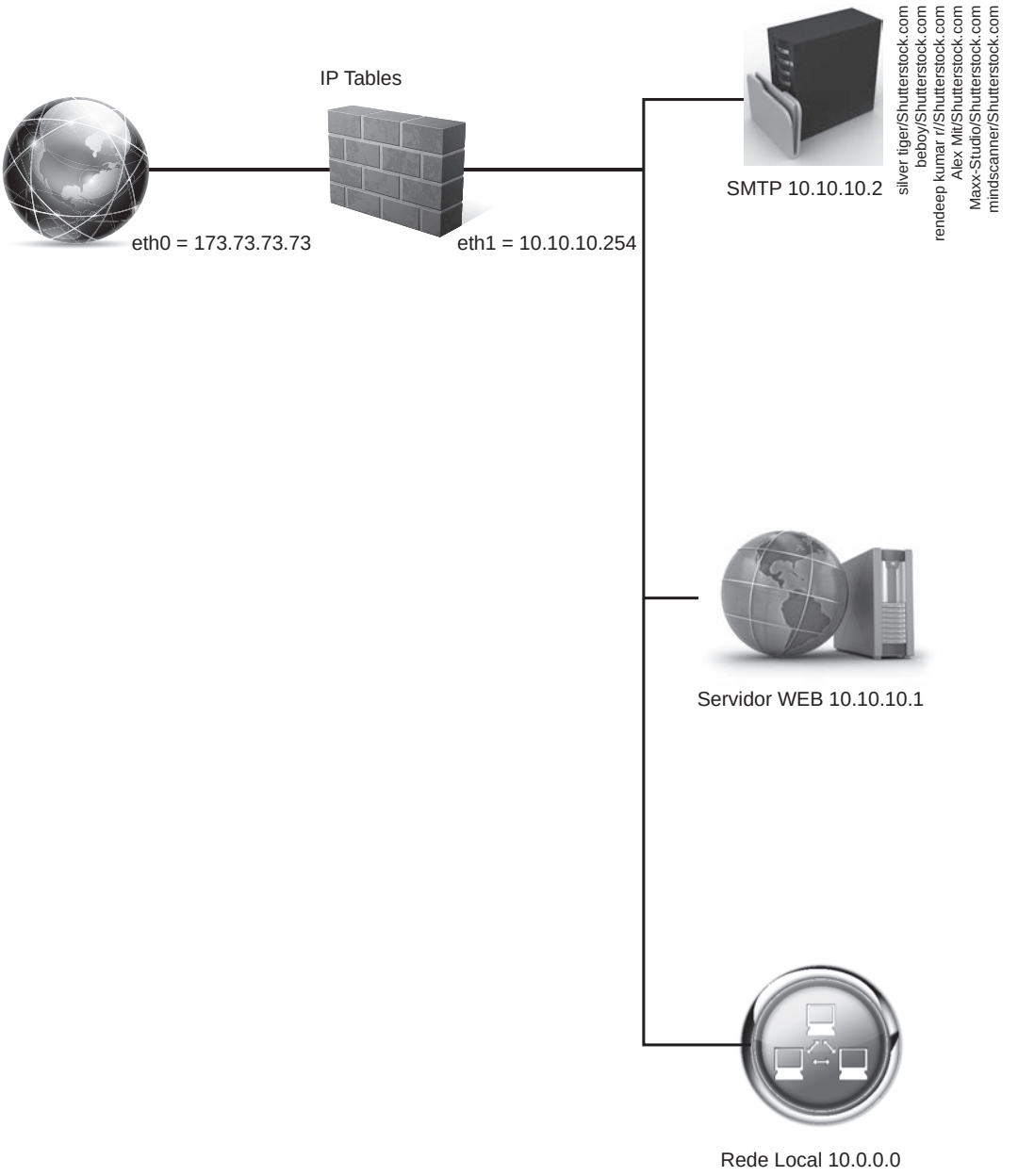


Figura 6.9 – Arquitetura de rede da empresa.

6.6.1 Passo a passo da configuração

» 1.º passo: vamos criar uma regra para bloquear todo o tráfego de rede da rede externa para a rede interna. Depois, criamos exceções de tráfego.

```
# iptables -P INPUT DROP

# iptables -P FORWARD DROP

# iptables -P OUTPUT ACCEPT
```

O tráfego de saída, ou seja, aquele proveniente da rede interna para a Internet, é válido e será permitido.

» 2.º passo: criando as regras de NAT estático.

Os servidores que iremos utilizar estão nos seguintes endereços:

10.10.10.1 – Servidor Web

10.10.10.2 – Servidor de Correio

Como o endereço público da rede externa é 173.73.73.73, teremos que criar as seguintes regras:

Regra para o servidor web:

```
# iptables -t nat -A PREROUTING -i eth0 -d 173.73.73.73 -m tcp -p tcp --dport
80 -j DNAT --to destination 10.10.10.1
```

Regra para o Servidor de Correio:

```
# iptables -t nat -A PREROUTING -i eth0 -d 173.73.73.73 -m tcp -p tcp -dport 25
-j DNAT -to destination 10.10.10.2
```

Regra para o NAT de retorno:

```
# iptables -t nat -A POSTROUTING -o eth0 -s 10.10.10.0/24 -j SNAT -- to source
173.73.73.73
```

» 3.º passo: liberando o acesso aos servidores.

```
# iptables -A FORWARD -i eth0 -d 10.10.10.1 -m tcp -p tcp --dport 80 -m state
---state NEW -j ACCEPT

# iptables -A FORWARD -i eth0 -d 10.10.10.2 -m tcp -p tcp -- dport 25 -m state
--state NEW -J ACCEPT
```

» 4.º passo: criando as regras para os usuários internos acessarem a Internet.

Para isso, adicionamos uma regra permitindo apenas o acesso a páginas web.

```
# iptables -A FORWARD -i eth1 -s 10.0.0.0/8 -m tcp -p tcp -- dport 80 -m state
- state NEW -j ACCEPT
```

» 5.º passo: criando regras para bloqueio de Facebook e YouTube.

```
# iptables -A OUTPUT -p tcp -- dport 80 -d www.facebook.com -j DROP

# iptables -A OUTPUT -p tcp -- dport 80 -d www.youtube.com -j DROP
```

» 6.º passo: agora criamos as regras para bloquear o tráfego peer to peer dos aplicativos Kazaa e ARES.

```
# iptables -A FORWARD -p tcp -m ipp2p -- kazaa -j DROP
# iptables -A FORWARD -p udp -m ipp2p - kazaa -j DROP
```

» 7.º passo: bloqueio de tráfego ICMP

```
# iptables -A INPUT -p ICMP -- icmp_type echo-request -j DROP
```

Vamos recapitular?

Neste capítulo aprendemos conceitos sobre o NetFilter e o IP Tables (como funcionam, suas funções, como trabalha o NAT) e apresentamos um exemplo de configuração.

Agora é com você!

1) Qual a principal finalidade de um filtro de pacotes?
2) Qual a capacidade de inspeção que o IP Tables possui que o caracteriza como uma importante ferramenta?
3) Qual a vantagem do IP Tables sobre firewalls proprietários?
4) O que é NAT estático? Como ele é utilizado?
5) O que é PAT ("Port Address Translation")?

6) Qual o número mínimo de endereços públicos com que podemos trabalhar com o PAT?

7) Quando as regras de NAT para acesso a servidores internos devem ser aplicadas no prerouting ou no postrouting? Por quê?

8) Quais as portas utilizadas pelas aplicações web e correio? Em quais versões do Linux o IP Tables normalmente já vem instalado?

9) Apresente as vantagens e desvantagens do uso do IP Tables em relação ao uso de um firewall proprietário.

7

Case de Aplicação e Projeto

Para começar

Neste capítulo vamos simular o trabalho de um consultor de segurança da informação na definição da arquitetura, das políticas de segurança, da implementação, da validação e dos testes de um projeto. O objetivo é aplicarmos os conceitos desenvolvidos nos capítulos anteriores do livro, com base em implementações de software livre.

7.1 Metodologia utilizada

Walt Disney foi um empreendedor visionário, um grande animador e produtor de filmes que criou um império conhecido como Walt Disney Company. Ele possuía uma filosofia de vida inovadora para o seu tempo, que se refletiu no sucesso dos seus negócios.

No final dos anos 1940, Walt Disney começou a planejar o seu primeiro grande parque temático. Conhecido como Disneylândia, foi inaugurado na Califórnia em 1955 e imediatamente tornou-se um sucesso. No início dos anos 1960, Disney comprou uma imensa área de terra no estado da Flórida com o objetivo de criar um parque muito maior do que a Disneylândia. Esse parque (na verdade, um imenso complexo de entretenimento) ficaria conhecido como Disney World.

Autor desconhecido/NASA

Figura 7.1 – Walt Disney.

No âmbito do Disney World, existia também o plano de se criar um parque para adultos, com atrações representando os principais países de mundo. Surge, então, o projeto do Epcot Center. Disney, no entanto, veio a falecer no ano de 1966, e não viu nenhum desses dois projetos concluídos.

O Disney World foi inaugurado formalmente em 1971, mas o Epcot Center, apenas em 1982. Quando da inauguração do Walt Disney World, a imprensa perguntou à filha de Disney, Diane Marie Disney, o que ela achava do legado que seu pai havia deixado com o novo parque, ainda que não houvesse tido a oportunidade de ver o resultado final (afinal, havia falecido 5 anos antes).

Diane, todavia, respondeu rapidamente que sim, seu pai já havia visto tudo aquilo antes. Mas como? A resposta a essa pergunta envolve a chamada Metodologia Disney.

É justamente essa metodologia que adotaremos para desenvolver nosso projeto de segurança. Mas, afinal, o que é a metodologia Disney?

A metodologia Disney se baseia na ideia de que devemos imaginar o projeto já pronto mesmo antes de começarmos a desenvolvê-lo. Disney criou esse método quando planejava suas animações, todas elas muito bem-sucedidas, como a do ratinho Mickey. A metodologia prega: "Imagine que o projeto já esteja pronto e faça as perguntas de trás para a frente." Como assim? Vamos às perguntas:

» O que está funcionando bem no projeto?

» O que está funcionando mal?

» Qual os desafios envolvidos no uso da tecnologia?

» As demandas foram atendidas?

» O desempenho está adequado?

» A solução superou as expectativas?

» O cliente ficou feliz com os resultados?

A partir dessa e de outras séries de questões, podemos criar os requisitos com boa expectativa de acerto e vislumbrar o que o cliente definitivamente espera do projeto. Disney sempre acreditou que o sucesso estava em atender e superar as expectativas dos clientes.

7.2 Consultoria – questionário do projeto

Vamos começar o nosso projeto elaborando um trabalho consultivo que usa a metodologia de Disney. Para isso, iniciemos respondendo a algumas questões direcionadas ao nosso cliente fictício.

» Questão 1: Você está satisfeito com a solução?

Resposta: Sim, a solução atende plenamente à nossa demanda.

» Questão 2: Que indicadores você tem para afirmar que a solução está adequada?

O número de casos de suporte baixou muito após a implementação da solução. Ademais, a rede está mais estável e mais confiável, por isso, nossos funcionários nos dizem que há uma percepção de melhoria. Antes, recebíamos pelo menos uma notificação por mês de ataques originados de nossa rede, mas a solução já está instalada há mais de três meses e não houve nenhuma notificação desde então.

Por diversas vezes fomos obrigados a pedir que o provedor mudasse nosso endereço IP, pois entrávamos em listas negras da Internet como spammers ou donos de domínios que enviam spams, e isso não ocorre mais.

» Questão 3: E quanto ao acesso dos usuários às páginas da Internet? Está adequado?

Sim, percebemos uma melhoria significativa quando implementamos as listas de filtros de bloqueios de sites, em especial quando bloqueamos os acessos às redes sociais. Houve um ganho muito grande de produtividade após a implantação desse processo. Ficamos um tempo monitorando e percebemos que havia empregados que ficavam horas navegando em sites não adequados, como Facebook, LinkedIn, Twitter... Além disso, identificamos e punimos funcionários que acessavam sites pornográficos no meio do expediente.

» Questão 4: O processo de manutenção da solução é eficiente?

A configuração por linha de comandos garante muita agilidade. Nossos operadores podem mudar as regras em segundos, aumentando nossa eficiência. O processo que tínhamos antes, com uma interface GUI para configuração, era muito demorado. Porém, sentimos falta de uma interface gráfica em que pudéssemos visualizar os logs. Isso seria um ponto de melhoria.

» Questão 5: E quanto ao controle do uso de FTP e downloads de arquivos? Houve melhora?

Sim, a adoção de políticas para restringir o uso do FTP trouxe uma melhoria muito grande, em especial para evitar que baixássemos arquivos infectados ou software pirata, o que representa um grande risco para a companhia.

» Questão 6: Falando em software pirata, como está funcionando o controle de aplicações do tipo P2P, como Kazaa e ARES?

Muito bem. Inicialmente, adotamos essas regras apenas como medida de monitoramento, mas nos espantamos ao verificar como essas ferramentas eram utilizadas internamente na rede, principalmente para baixar filmes. Após a implementação, tivemos uma melhoria

considerável de tempo de resposta e de utilização do link de comunicação, além de descobrirmos que quase 40% do link era utilizado com tráfego P2P.

» Questão 7: A solução atendeu a toda rede e aos usuários?

Sim, atendeu às 300 estações de rede, aos 10 servidores e às aplicações, portanto, toda a infraestrutura ficou protegida.

» Questão 8: Quanto ao endereçamento das estações, o projeto atendeu às expectativas?

Sim, criamos uma rede para os servidores (DMZ) e uma rede local para atender às estações, implementamos uma política de NAT estático para os servidores e para o proxy. O resultado foi bem satisfatório.

» Questão 9: A solução foi enxuta e de baixo custo?

Sim, a empresa decidiu adotar soluções de software livre. Assim sendo, implementamos um filtro de pacotes baseado no IP Tables. Adicionalmente, para controlar os acessos dos usuários à Internet, implementamos um proxy Squid, que faz proxy das conexões e controla os acessos dos usuários. Dessa maneira, protegemos a empresa também mascarando os acessos dos usuários, uma vez que estes não possuem roteamento à Internet, apenas por intermédio do proxy. Também foi implementado um serviço de DNS interno ao proxy.

Por sua vez, a solução para o roteamento foi igualmente adequada. Na verdade, mantivemos o roteamento no nosso roteador de borda, e a máquina do IP Tables simplesmente possuía uma rota estática para o roteador de borda que tomava as decisões de roteamento.

» Questão 10: A solução de cache foi adequada?

Sim, tivemos um ganho substancial no acesso à rede. Como nossos usuários normalmente acessam um número limitado de páginas, a utilização do cache nos trouxe um ganho substancial de performance.

» Questão 11: Os serviços disponíveis foram adequados?

Sim, basicamente permitimos o acesso da Internet ao nosso servidor web, ao tráfego de correios e a um servidor FTP corporativo. Para usuários internos liberamos apenas acessos HTTP, HTTPS e FTP, porém controlados pelo nosso proxy Squid.

» Questão 12: Qual foi a política aplicada para o resto do tráfego?

Tomamos a decisão de bloquear qualquer tráfego não autorizado. Assim sendo, as regras de firewall bloqueiam todo o tráfego que não for necessário à rede da empresa.

» Questão 13: Qual foi a arquitetura de segurança utilizada?

Escolhemos proteger o perímetro utilizando um firewall IP Tables com três interfaces, uma interface externa, uma interface interna e a interface de DMZ (Zona Desmilitarizada). Nosso proxy foi implementado na rede interna.

Na Figura 7.2 podemos observar o desenho dessa arquitetura.

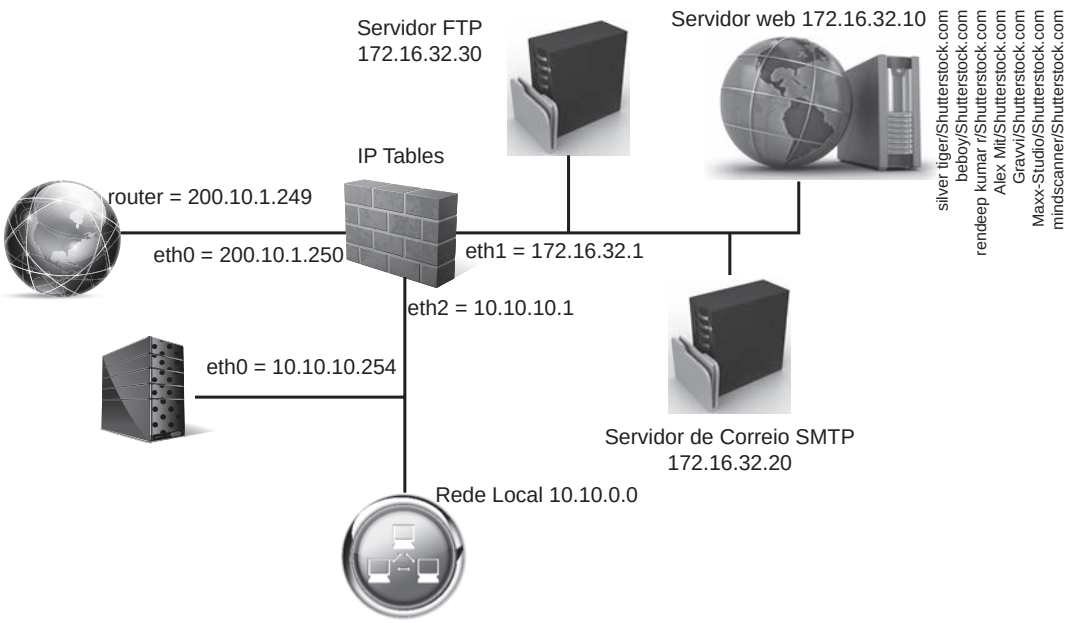


Figura 7.2 – Arquitetura da solução.

» Questão 14: Qual foi o endereçamento escolhido?

Contratou-se um serviço de acesso IP com uma rede classe C/29, que nos disponibilizou seis endereços IP válidos na subrede 200.10.1.248/29.

Os endereços válidos são:

» 200.10.1.249 – será utilizado na porta LAN do roteador;

» 200.10.1.250 – endereço IP válido disponível;

» 200.10.1.251 – endereço IP válido disponível;

» 200.10.1.252 – endereço IP válido disponível;

» 200.10.1.253 – endereço IP válido disponível;

» 200.10.1.254 – endereço IP válido disponível.

Foi feito um NAT estático dos servidores que estão na DMZ, e a tabela de NAT pode ser observada a seguir.

Tabela 7.1 – NAT estático

Endereço IP válido	Porta	Endereço IP privado	Porta
200.10.1.251	80	172.16.32.10	80
200.10.1.252	25	172.16.32.20	25
200.10.1.253	20/21	172.16.32.30	20/21

Para os usuários da rede interna vamos fazer um NAT estático entre o endereço do proxy e o endereço IP válido 200.10.1.254. Não será permitida nenhuma conexão originada da rede externa para o endereço IP do proxy. Todas as conexões internas passaram pelo proxy, o qual passará pelo processo de NAT.

Tabela 7.2 – Conexões internas

Endereço IP Privado	Porta	Endereço IP válido	Porta
10.10.10.254	80	200.10.1.254	80
10.10.10.254	435	200.10.1.254	435
10.10.10.254	20/21	200.10.1.254	20/21

7.3 Desenvolvimento do projeto

Podemos observar que a grande vantagem da metodologia Disney é nos oferecer uma total visibilidade do que é o projeto e qual a expectativa do cliente. Isto é, temos uma boa ideia do que o cliente espera, inclusive em termos de topologia. Muitas vezes esse questionário é respondido de forma induzida pelo consultor, especialmente quando ele ainda não tem ideia de como seria o projeto.

Mesmo assim, já temos um leque poderoso de informações e uma arquitetura bem-definida.

O próximo passo é definir as listas de acesso. Para isso, vamos fazer uma tabela de acessos, que será a base para a implementação da política na próxima fase.

Tabela 7.3 – Acessos

Regra	Acesso De	Porta Origem	Acesso Para	Porta Destino	Política	Política
# 1	INTERNET	Aleatória	200.10.1.251	80	Aplicar NAT para servidor web endereço 172.16.32.10 porta 80	Permitir
# 2	INTERNET	Aleatória	200.10.1.252	25	Aplicar NAT para servidor de correio endereço 172.16.32.20 porta 25	Permitir
# 3	INTERNET	Aleatória	200.10.1.253	20/21	Aplicar NAT para servidor FTP endereço 172.16.32.30 porta 20/21	Permitir
# 4	INTERNET	Aleatória	Rede 200.10.1.x	Aleatória	Não aplica NAT	Bloqueia
# 5	PROXY 10.10.10.254	Aleatória	172.16.32.10	80	Não aplica NAT – acesso da rede Interna a servidores	Permite
# 6	PROXY 10.10.10.254	Aleatória	172.16.32.30	20/21	Não aplica NAT – acesso da rede Interna a servidores	Permite
# 7	PROXY 10.10.10.254	Aleatória	INTERNET	80	Aplica NAT alterando o endereço de origem para 200.10.1.254 (aplicar restrições do Squid)	Permite
# 8	PROXY 10.10.10.254	Aleatória	INTERNET	20/21	Aplica NAT alterando o endereço de origem para 200.10.1.254 (aplicar restrições do Squid)	Permite
# 9	PROXY 10.10.10.254	Aleatória	INTERNET	435	Aplica NAT alterando o endereço de origem para 200.10.1.254 (aplicar restrições do Squid)	Permite
# 10	REDE LOCAL 10.10.X.X	Aleatória	INTERNET	Aleatória	Não aplica NAT, tráfego não permitidoa deve-se restringir o acesso da interface do IP Tables apenas ao proxy	Bloqueia
# 11	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	2138	Permitido, o IP Tables não tem como negar esse tráfego porque está na rede interna, os acessos serão configurados no Squid	Permite
# 12	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	Porta FTP	Permitido, o IP Tables não tem como negar esse tráfego porque está na rede interna, os acessos serão configurados no Squid	Permite

Regra	Acesso De	Porta Origem	Acesso Para	Porta Destino	Política	Política
# 13	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	SLL	Permitido, o IP Tables não tem como negar esse tráfego porque está na rede interna, os acessos serão configurados no Squid	Permite
# 14	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	Aleatória	Será bloqueado pelo Squid, normalmente portas não abertas não estão em Listening e a conexão não se completa	Bloqueia

7.4 Implementação das políticas

Inicialmente, vamos trabalhar com a configuração do IP Tables, que será o nosso firewall de perímetro.

```
# iptables –P INPUT DROP
# iptables –P FORWARD DROP
# iptables –P OUTPUT ACCEPT
```

Os servidores que iremos utilizar estão nos seguintes endereços:

- 172.16.32.10 – Servidor web e endereço público de NAT: 200.10.1.251
- 172.16.32.20 – Servidor de correio e endereço público de NAT: 200.10.1.252
- 172.16.32.30 – Servidor de FTP e endereço público de NAT: 200.10.1.253
- 10.10.10.254 – Proxy Server e endereço público de NAT: 200.10.1.254

Regra para o servidor web:

```
# IPTABLES -t nat -A PREROUTING –i eth0 -d 200.10.1.251 –m tcp –p tcp –dport 80 -j DNAT
--to destination 172.16.32.10
```

Regra para o servidor de correio:

```
# IPTABLES -t nat -A PREROUTING –i eth0 -d 200.10.1.252 –m tcp –p tcp –dport 25 -j DNAT
--to destination 172.16.32.20
```

Regra para o servidor FTP:

```
# IPTABLES -t nat -A PREROUTING –i eth0 -d 200.10.1.253 –m tcp –p tcp –dport 20 -j DNAT
--to destination 172.16.32.30
# IPTABLES -t nat -A PREROUTING –i eth0 -d 200.10.1.253 –m tcp –p tcp –dport 21 -j DNAT
--to destination 172.16.32.30
```

Regra para o servidor proxy:

```
# IPTABLES -t nat -A PREROUTING –i eth0 -d 200.10.1.254 -j DNAT --to destination
10.10.10.254
```

Regra para o NAT de retorno:

```
# iptables –t nat –A POSTROUTING –o eth2 –s 10.10.10.254 –j SNAT -- to source
200.10.1.254
# iptables –t nat –A POSTROUTING –o eht1 –s 172.16.32.10 –j SNAT -- to source
200.10.1.251
# iptables –t nat –A POSTROUTING –o eht1 –s 172.16.32.20 –j SNAT -- to source
200.10.1.252
# iptables –t nat –A POSTROUTING –o eht1 –s 172.16.32.30 –j SNAT -- to source
200.10.1.253
```

Liberando o acesso aos servidores:

```
# iptables –A FORWARD –i eth0 –d 172.16.32.10 –m tcp –p tcp --dport 80 –m state ---state
NEW –j ACCEPT
# iptables –A FORWARD –i eth0 –d 172.16.32.20 –m tcp –p tcp -- dport 25 –m state --state
NEW –J ACCEPT
# iptables –A FORWARD –i eth0 –d 172.16.32.30 –m tcp –p tcp -- dport 20 –m state --state
NEW –J ACCEPT
# iptables –A FORWARD –i eth0 –d 172.16.32.30 –m tcp –p tcp -- dport 21 –m state --state
NEW –J ACCEPT
```

Criando as regras para os usuários pelo proxy:

```
 # iptables –A FORWARD –i eth1 –s 10.10.10.254 –m tcp –p tcp -- dport 80 –m state – state
NEW –j ACCEPT
# iptables –A FORWARD –i eth1 –s 10.10.10.254 –m tcp –p tcp -- dport 435 –m state – state
NEW –j ACCEPT
# iptables –A FORWARD –i eth1 –s 10.10.10.254 –m tcp –p tcp -- dport 20 –m state – state
NEW –j ACCEPT
# iptables –A FORWARD –i eth1 –s 10.10.10.254 –m tcp –p tcp -- dport 21 –m state – state
NEW –j ACCEPT
```

Criando regras para bloqueio de Facebook, LinkedIn e Twitter:

```
# iptables –A OUTPUT –p tcp -- dport 80 –d www.facebook.com -j DROP
# iptables –A OUTPUT –p tcp -- dport 80 –d www.linkedin.com -j DROP
# iptables –A OUTPUT –p tcp -- dport 80 –d www.twitter.com -j DROP
```

Vamos criar regras para bloquear o tráfego peer to peer dos aplicativos Kazaa e ARES:

```
# iptables –A FORWARD –p tcp –m ipp2p -- kazaa –j DROP
# iptables –A FORWARD –p udp –m ipp2p – kazaa –j DROP
```

Bloquear tráfego ICMP:

```
# iptables –A INPUT –p ICMP -- icmp_type echo-request –j DROP
```

Agora vamos fazer a configuração do Squid.

```
http_port 3128
refresh_pattern ^ftp:           1440    20%     10080
```

```
refresh_pattern ^gopher:        1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0     0%      0
refresh_pattern .               0       20%     4320

acl localnet src 10.0.0.0/8     # RFC 1918 possible internal network
acl localnet src 172.16.0.0/12  # RFC 1918 possible internal network
acl localnet src 192.168.0.0/16 # RFC 1918 possible internal network

acl SSL_ports port 443          # https

acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http

acl CONNECT method CONNECT

http_access deny !Safe_ports
http_access deny CONNECT !SSL_ports
http_access allow localhost manager
http_access deny manager
http_access allow localnet
http_access allow localhost
http_access deny all
```

Vamos bloquear os sites no Squid também.

Criar o arquivo sitesbloqueados.squid

Executar o comando #cat /etc/squid/sitesbloqueados.squid

```
# sites bloqueados
www.twitter.com
www.linkedin.com
www.facebook.com
```

Vamos editar o arquivo /etc/squid/squid.conf e criar uma nova ACL apontando para o arquivo sitesbloqueados.squid

```
acl bloquearsites dstdomain "/etc/squid/sitesbloqueados.squid"
```

Agora, criamos uma linha com o http_access para bloquear o acesso:

```
http_access deny bloquearsites
```

Vamos reiniciar o serviço

```
Service squid restart
```

```
# bloquear palavras
Emprego
XXX
Porn
```

Vamos abrir o arquivo /etc/squid/squid.conf e criar uma ACL bloquear_palavras

```
Acl bloquear_palavras url_regex -i "/etc/squid/bloquearpalavras.squid"
```

Vamos criar a regra http_access para bloquear palavras

```
http_access deny bloquear_palavras
```

Vamos agora configurar o cache do Squid

```
Cache_mem 800 MB
Maximum_object_size_in_memory 32kb
Maximum_object_size 1024 MB
Minimum_object_size 0 Kb
Cache_swap_low 90
```

7.5 Testes

O próximo passo é realizar os testes das tabelas de acesso e verificar se tudo está funcionando.

Plano de testes:

7.5.1 Regra 1

# 1	INTERNET	Aleatória	200.10.1.251	80	Aplicar NAT para servidor web endereço 172.16.32.10 porta 80	Permitir

Para testar essa regra, o melhor é conseguirmos uma conexão externa com um modem 3G e tentar fazer um acesso ao servidor web.

» Critério de aceitação: receber a página do servidor corretamente, com um tempo de resposta adequado.

7.5.2 Regra 2

# 2	INTERNET	Aleatória	200.10.1.252	25	Aplicar NAT para servidor de correio endereço 172.16.32.20 porta 25	Permitir

Para testar essa regra, o melhor é verificar se os emails estão chegando. Envie um email a partir de uma conta externa (por exemplo, um Gmail ou Yahoo mail) e aguarde o recebimento.

» Critério de aceitação: o e-mail deve chegar corretamente.

7.5.3 Regra 3

# 3	INTERNET	Aleatória	200.10.1.253	20/21	Aplicar NAT para servidor FTP endereço 172.16.32.30 porta 20/21	Permitir

Para testar essa regra, o melhor é tentar se conectar no servidor de FTP e baixar um arquivo a partir de uma conexão externa, por exemplo, um modem 3G/4G.

» Critério de aceitação: o arquivo deve chegar da forma correta e não corrompido.

7.5.4 Regra 4

# 4	INTERNET	Aleatória	Rede 200.10.1.x	Aleatória	Não aplica NAT	Bloqueia

Para testar essa regra, o melhor a fazer é, por meio de um acesso externo (pode ser via modem 3G/4G) e do uso de uma ferramenta de segurança como o NMAP, executar o comando NMAP –S –O 200.10.1.252-254 e verificar se existem portas abertas que não estão sendo bloqueadas.

» Critério de aceitação: todas as portas não permitidas devem estar bloqueadas.

7.5.5 Regra 5

# 5	PROXY 10.10.10.254	Aleatória	172.16.32.10	80	Não aplica NAT – acesso rede interna a servidores	Permite

O objetivo dessa regra é verificar se a máquina do proxy consegue acessar a DMZ. Recomendamos tentar abrir a página do servidor da empresa a partir do proxy e ver se funciona. Caso não haja console gráfico ou navegador de Internet no Proxy, o teste pode ser feito com o comando telnet, executando-se telnet 172.16.32.10:80.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.6 Regra 6

# 6	PROXY 10.10.10.254	Aleatória	172.16.32.30	20/21	Não aplica NAT – acesso rede interna a servidores	Permite

O objetivo dessa regra é verificar se a máquina do proxy consegue acessar o servidor FTP da DMZ. Recomendamos abrir uma sessão de FTP a partir do proxy e ver se funciona. Caso não haja cliente de FTP no proxy, o teste pode ser executado com o comando telnet, executando-se telnet 172.16.32.10:20 e telnet 172.16.32.10:21.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.7 Regra 7

# 7	PROXY 10.10.10.254	Aleatória	INTERNET	80	Aplica NAT alterando o endereço de origem para 200.10.1.254 (aplicar restrições do Squid)	Permite

O objetivo dessa regra é verificar se a máquina do proxy consegue acessar a web. Recomendamos tentar abrir uma página na Internet, o Google, por exemplo, a partir do proxy e ver se funciona. Caso não haja console gráfico ou navegador de Internet no proxy, o teste pode ser feito com o comando telnet, executando-se telnet www.google.com:80.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.8 Regra 8

# 8	PROXY 10.10.10.254	Aleatória	INTERNET	20/21	Aplica NAT alterando o endereço de origem para 200.10.1.254 (aplicar restrições do Squid)	Permite

O objetivo dessa regra é verificar se a máquina do proxy consegue acessar um servidor FTP na Internet. Recomendamos tentar abrir uma sessão de FTP em algum FTP público na Internet, como ftp.microsoft.com.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.9 Regra 9

# 9	PROXY 10.10.10.254	Aleatória	INTERNET	435	Aplica NAT alterando o endereço de origem para 200.10.1.254 (aplicar restrições do Squid)	Permite

O objetivo dessa regra é verificar se a máquina do proxy consegue estabelecer uma conexão segura na Internet. Recomendamos tentar abrir uma página na Internet, o Google, por exemplo, a partir do proxy, mas usando a linha <https://www.google.com> – acessando-se, assim, o servidor seguro do Google – e ver se funciona. Caso não haja console gráfico ou navegador de internet no proxy, o teste pode ser feito com o comando telnet, executando-se telnet <www.google.com:435>.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.10 Regra 10

# 10	REDE LOCAL 10.10.X.X	Aleatória	INTERNET	Aleatória	Aplica NAT, tráfego não permitido, deve-se restringir o acesso da interface do IP Tables apenas ao proxy	Bloqueia

O objetivo dessa regra é evitar que máquinas internas consigam acessar a internet sem que isso seja efetuado por meio do proxy. Para testar a regra, recomendamos eliminar a configuração de proxy do browser e verificar se a navegação ainda é possível.

» Critério de aceitação: a conexão não deve ser estabelecida, isto é, a máquina não deve conseguir acessar a Internet se isso não for feito por meio do browser.

7.5.11 Regra 11

# 11	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	2138	Permitido, o IP Tables não tem como negar esse tráfego porque está na rede interna, os acessos serão configurados no Squid	Permite

O objetivo aqui é verificar se os clientes da rede local têm acesso à máquina do proxy. Esse teste pode ser feito simplesmente executando-se um telnet 10.10.25: 2138, verificando-se, então, se a mesma está aberta.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.12 Regra 12

# 12	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	Porta FTP	Permitido, o IP Tables não tem como negar esse tráfego porque está na rede interna, os acessos serão configurados no Squid.	Permite

O objetivo agora é verificar se os clientes da rede local têm acesso à máquina do proxy no serviço de FTP. Esse teste pode ser feito simplesmente executando-se um telnet 10.10.25: 20 e 21, verificando-se, então, se a mesma está aberta.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.13 Regra 13

# 13	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	SLL	Permitido, o IP Tables não tem como negar esse tráfego porque está na rede Interna, os acessos serão configurados no Squid.	Permite

O objetivo desta feita é verificar se os clientes da rede local têm acesso à máquina do proxy no serviço de SSL. Esse teste pode ser feito simplesmente executando-se um telnet 10.10.25: 435, verificando-se, então, se a mesma está aberta.

» Critério de aceitação: a conexão deve ser estabelecida.

7.5.14 Regra 14

# 14	REDE LOCAL 10.10.X.X	Aleatória	PROXY 10.10.10.254	Aleatória	Será bloqueado pelo Squid, normalmente portas não abertas não estão em Listening e a conexão não se completa	Bloqueia

A ideia é que a máquina do proxy não tenha portas abertas que não aquelas esperadas dos próprios serviços de proxy. Podemos novamente usar o aplicativo NMAP para verificar as portas abertas, executando o comando NMAP –S –O 10.10.10.254. Então, verifique se existem portas abertas que não estejam sendo bloqueadas.

» Critério de aceitação: todas as portas não permitidas devem estar bloqueadas.

Vamos recapitular?

Neste capítulo apresentamos a metodologia Disney e mostramos como ela pode nos apoiar em um projeto modelo. Usamos os dados obtidos com o cliente e foi possível montar um projeto lógico, um projeto de endereçamento IP, um projeto de NAT e as políticas de acesso para implementação tanto no firewall de borda, o IP Tables, como no proxy.

Agora é com você!

1) Um projeto sempre precisa refletir a realidade e os requisitos do cliente. Qual foi o método utilizado neste capítulo?

2) Por que consideramos que Walt Disney quebrou um paradigma quando idealizou os seus parques temáticos da Flórida, mesmo sem ter tido a oportunidade de estar na sua inauguração?

3) Qual foi a estratégia de NAT utilizada em todo o projeto. Por quê?

4) Por que implantamos regras de bloqueio de tráfego peer to peer? Qual o maior benefício que o cliente espera com esse trabalho?

5) Qual o objetivo do controle no acesso à Internet? O que se espera com isso?

6) Por que é interessante bloquear o tráfego ICMP?

7) Qual a faixa de endereçamento privado utilizada na DMZ? Não seria mais fácil mantermos endereços públicos na DMZ?

8) Existe roteamento direto das máquinas da rede local para a Internet? Quem atua nesse bloqueio?

9) Qual o objetivo do bloqueio às redes sociais?

10) O que acontece se o serviço do proxy falhar? Que melhorias você proporia para esse projeto?

Bibliografia

ABDEL-AZIZ, A. **Intrusion Detection & Response Leveraging Next Generation Firewall Technology**. 19 fev. 2009. Disponível em: <http://www.sans.org/reading-room/whitepapers/firewalls/intrusion-detection-response-leveraging-generation-firewall-technology-33053>. Acesso em: 18 fev. 2015.

ABOUT LINUX. **Linux/Unix Command**: iptables. Disponível em: <http://linux.about.com/od/commands/l/blcmdl8_iptable.htm>. Acesso em: 17 fev. 2015.

ALMEIDA, M. B. **Introdução ao iptables**. Disponível em: <http://pt.slideshare.net/marcelobarrosalmeida/tutorial-sobre-iptables>. Acesso em: 10 fev. 2015.

CARY, K. **Case study of analysis methods for firewall retrofit and operation at ABC University**. 30 ago. 2006. Disponível em: <http://www.sans.org/reading-room/whitepapers/firewalls/firewall-analysis-operation-methods-1659>. Acesso em: 15 fev. 2015.

CASALICCHIO, C. A. A. **Aplicando a Metodologia Disney no Brasil**. 2014. Disponível em: <http://www.ccasalicchio.com/wp-content/uploads/2014/05/Aplicando-a-Metodologia-Disney-no-Brasil.pdf>. Acesso em: 20 fev. 2015.

CHADWICK, D. **W. Network firewall technologies**. Disponível em: <http://alphasecurenetworks.com/wp-content/uploads/2013/01/network-firewall-technologies.pdf>. Acesso em: 21 fev. 2015.

CIRONE, A. C.; MORAES, A. F. **Redes de Computadores da Ethernet à Internet**. São Paulo: Érica, 2004.

COLE, E. **Real-world testing of next-generation firewalls**. out. 2013. Disponível em: <http://www.sans.org/reading-room/whitepapers/analyst/real-world-testing-next-generation-firewalls-34955>. Acesso em: 22 fev. 2015.

INTERNET FAQ ARCHIVE. **Drawbacks with restore**. Disponível em: <http://www.faqs.org/docs/iptables/drawbackswithrestore.html>. Acesso em: 12 fev. 2015.

JONES, A. **Netfilter and IPTables:** A Structural Examination. 26 fev. 2014. Disponível em: <http://www.sans.org/reading-room/whitepapers/firewalls/netfilter-iptables-structural-examination-1392>. Acesso em: 11 fev. 2015.

LINUX TODAY. **Working with iptables**. Disponível em: <http://www.linuxtoday.com/upload/working-with-iptables-121126061011.html>. Acesso em: 15 fev. 2015.

MICROSOFT. **Install and Configure ISA Server 2006 or Other Firewall**. Disponível em: <https://technet.microsoft.com/en-us/library/cc182268.aspx>. Acesso em: 8 fev. 2015.

MORAES, A. F. **Segurança em Redes** – Fundamentos. São Paulo: Érica 2010.

NETFILTER. **What is netfilter.org?** Disponível em: <http://www.netfilter.org/index.html>. Acesso em: 13 fev. 2015.

SCHRODER, C. **Building firewalls with iptables, part 2**. 10 jun. 2003. Disponível em: <http://www.enterprisenetworkingplanet.com/netsecur/article.php/2219571/Building-Firewalls-with-iptables-Part-2.htm>. Acesso em: 16 fev. 2015.

SERVIN, S. **Microsoft ISA Server, Part I:** introduction, installation, configuration, Web caching and Internet access. Windows Security. Disponível em: <http://www.windowsecurity.com/articles-tutorials/firewalls_and_VPN/Microsoft_ISA_Server_Part_I__introduction_installation_configuration_Web_caching_and_Internet_access.html>. Acesso em: 8 fev. 2015.

SHARMA, B.; BAJAJ, K. Packet Filtering using IP Tables in Linux. **IJCSI International Journal of Computer Science Issues,** v. 8, Issue 4, n. 2, July 2011. Disponível em: <http://ijcsi.org/papers/IJCSI-8-4-2-320-325.pdf>. Acesso em: 15 fev. 2015.

VIVA O LINUX. **Linux - Squid.** Disponível em: <http://www.vivaolinux.com.br/artigos/verSubCategoria.php?codigo=101>. Acesso em: 19 fev. 2015.