Unidade V

5 DISPOSITIVOS DE SEGURANÇA PARA REDES

Segundo Beal (2005, p. 93), as preocupações com a segurança da rede

> [...] devem abranger os problemas de autenticação de usuários e equipamentos e de restrição de acesso dos usuários aos serviços autorizados, contemplando o estabelecimento de interfaces seguras entre a rede interna e as redes públicas ou de outras organizações.

Os elementos básicos para a proteção de rede incluem dispositivos como roteadores de borda, firewalls, NAT (network address translation), VPN (virtual private network), bastion host, perímetro lógico, IDS (intrusion detection system), IPS (intrusion prevention system) e políticas de segurança.

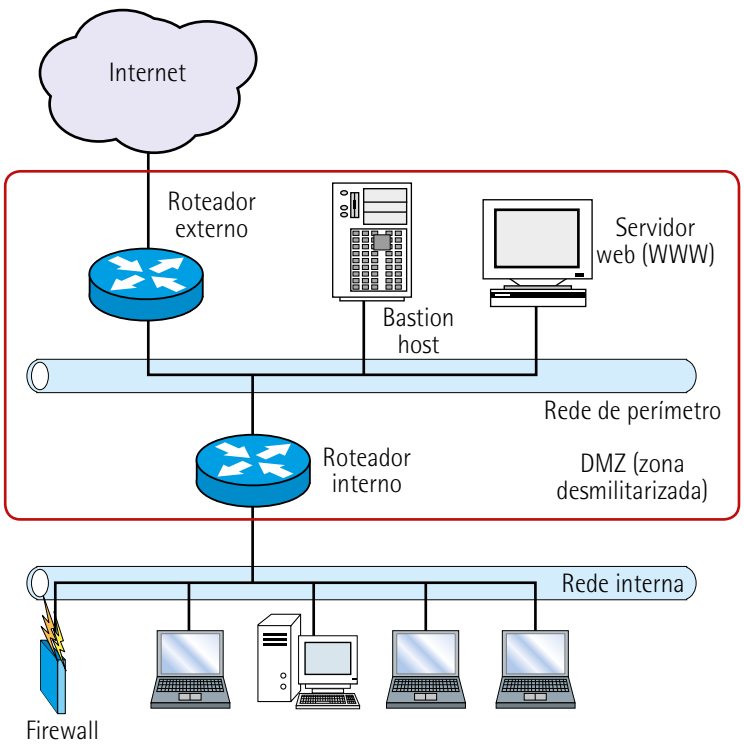

Figura 15 – Elementos básicos de controle de acesso a redes

5.1 Roteador de borda e NAT

O roteador de borda é o último gateway que conecta a rede interna da empresa à internet. Segundo Ramos (2008), é a primeira linha de defesa da empresa contra ameaças externas, um elemento fundamental para a composição de diversos sistemas de firewall. No entanto, é bastante comum que

não seja utilizado para funções de segurança, e isso por dois motivos. O primeiro é o fato de que, muitas vezes, esse roteador não pertence à organização, e sim às empresas que proveem a conexão com a internet. O segundo motivo diz respeito a sua dificuldade de configuração, normalmente feita via linha de comando, o que leva muitos administradores, por questão de praticidade, a abrir mão desse recurso fundamental.

Esse roteador facilita criar um controle de acesso. Desempenhando o papel de filtro, gera listas de acesso (ou ACLs), as quais costumam ser classificadas como **filtros de pacotes simples**. Em geral, as listas de acesso são configuradas para permitir ou negar determinado tipo de tráfego, levando em consideração as informações de endereço de origem e destino, portas de passagem e destino.

Por serem equipamentos que trabalham na camada 3, os roteadores têm pouca ou nenhuma interferência quando comparados aos da camada 7 (de aplicação).

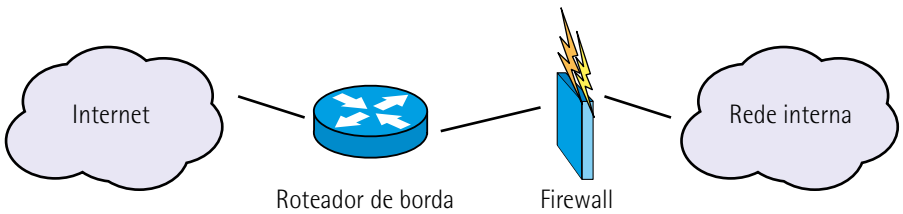

Figura 16 – Topologia com um roteador de borda

Observação

Cabe ressaltar que os roteadores de borda devem trabalhar sempre em conjunto com outros sistemas de defesa, como firewall, proxy, IDS e IPS.

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

O mapeamento entre endereços válidos e inválidos pode ser:

- **Único**: existe um único endereço inválido mapeado em um endereço válido.
- **Um para um**: para cada endereço inválido, deve existir um endereço válido.
- **Muitos para um**: muitos endereços inválidos compartilham o mesmo endereço válido. É o mais utilizado.

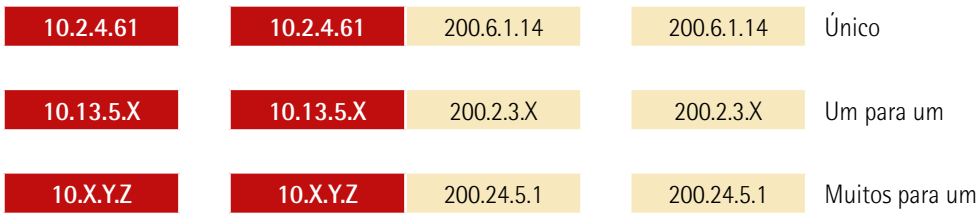

Figura 17 – Mapeamento dos endereços com NAT

A NAT foi concebida para permitir que máquinas acessem a internet sem necessariamente ter um endereço IP válido, já que os endereços válidos são centralmente distribuídos e controlados. Foram criadas faixas de endereçamento chamadas de **inválidas**, que podem ser usadas livremente sem a necessidade de reportar-se aos CGIs (Comitês Gestores da Internet), órgãos que controlam os endereços válidos de internet em cada país. No entanto, esses endereços "não existem" na internet real. É por isso que, quando um pacote sai de uma rede inválida para uma válida, ele precisa ter o endereço de origem alterado.

A NAT oferece benefícios do ponto de vista da segurança, pois normalmente máquinas não conseguem, a partir da internet, acessar de forma direta máquinas que estão na rede interna. Essa tecnologia permite o afunilamento do acesso à internet, em alguns pontos, pela rede interna. "Pelo fato de o firewall ser geralmente um gateway, ele pode desempenhar essas funções, que também se combinam com as funções de VPN para criar soluções de conectividade e segurança conjuntas" (RAMOS, 2008, p. 162).

O uso da NAT aumenta ainda mais a segurança da rede interna porque o endereço das estações fica mascarado.

5.2 Firewall e proxy

O firewall é um conjunto de hardware e software que permite criar regras quanto a que tipos de serviço e tráfego são permitidos entre as redes que ele conecta. É um dispositivo de controle de acesso, e sua função principal é a proteção das estações e a segmentação de perímetros. Costuma ser colocado na junção de duas redes com níveis de confiança distintos.

Em geral, é um computador independente (standalone), um roteador ou um firewall em uma caixa (dispositivo de hardware proprietário). A unidade serve como único ponto de entrada para o site de quem a utiliza, e avalia cada solicitação de conexão quando é recebida (a maioria dos firewalls faz isso verificando o endereço de origem). Somente as solicitações de equipamentos autorizados são processadas; as demais são descartadas.

Os firewalls podem analisar pacotes recebidos de vários protocolos. Com base nessa análise, empreendem várias ações. São, portanto, capazes de realizar avaliações condicionais ("Se esse tipo de pacote for encontrado, farei isso").

Essas construções condicionais são chamadas de **regras**. Em geral, ao ser configurado, o firewall é equipado com as regras que espelham as diretivas de acesso da organização que o utiliza.

Entretanto, a verificação de acesso é apenas uma parte do que os firewalls modernos são capazes de fazer. A maioria deles permite verificar o conteúdo. Pode-se explorar essa capacidade para bloquear Java, JavaScript, VBScript, scripts ActiveX e cookies. De fato, é possível criar regras para bloquear determinadas assinaturas de ataque.

Os componentes de um firewall baseiam-se na mente das pessoas que o desenvolvem. Em sua essência, é um conceito em vez de um produto; é uma ideia de quem terá permissão para acessar um site.

No sentido mais geral, o software de um firewall pode ser proprietário ou shareware, e o hardware pode ser qualquer um que suporte o software.

Os firewalls dividem-se em duas categorias básicas: firewalls de nível de rede e firewalls de gateway de aplicativo.

Os **firewalls de nível de rede** costumam ser roteadores com uma poderosa capacidade de filtragem de pacote. Por meio deles, pode-se conceder ou negar acesso a um site com base em diversas variáveis, como endereço de origem, protocolo, número de porta e conteúdo.

Os firewalls baseados em roteador são populares por serem facilmente implementados. Para conectar um, basta fornecer algumas regras. Além disso, a maioria dos roteadores novos faz um trabalho muito bom de tratamento de interfaces dúbias, quando IPs de fora devem ser traduzidos por algum protocolo interno.

Adicionalmente, um firewall baseado em roteador é uma solução de perímetro. Como os roteadores são dispositivos externos, eles eliminam a necessidade de interromper a operação normal da rede.

Os roteadores também oferecem uma solução integrada. Se sua rede estiver permanentemente conectada à internet, de qualquer maneira será necessário usar um roteador. Assim, é possível unir duas utilidades em uma.

No entanto, esse tipo de firewall tem várias deficiências. Muitos roteadores, por exemplo, são vulneráveis a ataques de personificação (spoofing), embora fornecedores já estejam desenvolvendo soluções para isso. Ademais, de um ponto de vista prático, o desempenho do roteador cai dramaticamente quando se impõem procedimentos de filtragem muito rigorosos.

Observação

Ataques de IP spoofing consistem na falsificação de endereços IP a fim de fazer uma rede direcionar o usuário para sites fraudulentos.

Os **firewalls de aplicativo proxy** são às vezes referidos como **gateways de aplicativo**. Quando um usuário remoto entra em contato com uma rede executando um gateway de aplicativo, este gerencia a conexão (proxies). Nesse caso, pacotes IP não são encaminhados à rede interna. Em vez disso, um tipo de tradução ocorre, com o gateway agindo como canal e intérprete.

A vantagem de gateways de aplicativo é que impedem o tunelamento de pacotes IP na rede, e sua desvantagem é que exigem overheads altos, envolvendo grande parte da rede. Um aplicativo proxy deverá ser configurado para cada serviço na rede, como FTP (file transfer protocol), Telnet, HTTP (hypertext transfer protocol) e correio. Adicionalmente, usuários internos deverão utilizar clientes de proxy e, nesse caso, será preciso adotar novas diretivas e novos procedimentos.

Para construir um firewall, é necessário seguir seis passos:

- Identifique a topologia, o aplicativo e as necessidades de protocolo.
- Analise os relacionamentos de confiança em sua organização.
- Desenvolva diretivas baseadas nas necessidades e nos relacionamentos.
- Identifique o firewall correto para sua configuração específica.
- Empregue esse firewall de maneira adequada.
- Teste suas diretivas rigorosamente.

Dos passos mencionados, podemos destacar o desenvolvimento de diretivas, a obtenção do firewall correto e o teste rigoroso das diretivas.

Para desenvolver diretivas, é preciso determinar quem acessa a rede e como. Também devem ser consideradas quaisquer informações específicas de plataforma ou de protocolo.

A partir dessas informações, é possível fazer uma escolha fundamentada sobre o tipo de firewall necessário. Sabendo-se o que é preciso, pode-se discutir a questão com vários fornecedores sem ficar exposto a enganações. Antes de conduzir uma pesquisa de aquisição, gere uma lista de itens obrigatórios. Em última instância, sua decisão se baseará nessa lista.

Depois de adquirido o firewall, é o momento de instalar e testar as diretivas. É recomendado fazer isso em duas fases, avaliando-se as diretivas impostas contra estranhos e as diretivas internas.

A primeira fase pode ser feita a qualquer hora, mesmo (e talvez preferencialmente) quando os usuários estão ausentes, como num fim de semana ou fora do horário de expediente.

A segunda fase é mais complicada. Espere muitos problemas e custos extras devido ao tempo de inatividade ou paralisação da rede (downtime). Além disso, fique preparado para se defrontar com

usuários zangados. É bastante improvável esse teste ser realizado corretamente na primeira vez, a menos que a rede seja totalmente homogênea e você tenha um conjunto consistente de aplicativos para todos.

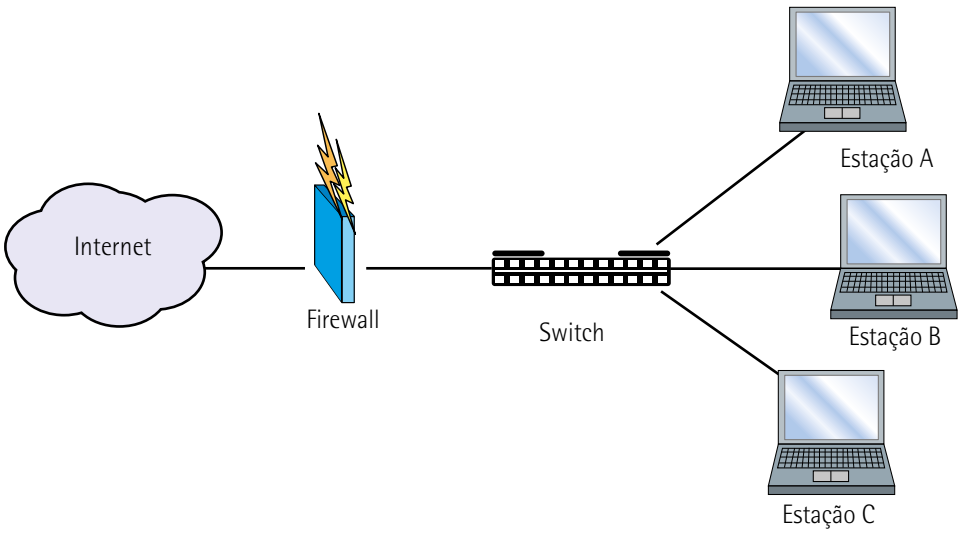

Figura 18 – Topologia com um firewall

De acordo com Ramos (2008), nos primórdios da internet, as primeiras iniciativas de proteção de redes conectadas ao mundo externo passaram pela tentativa de implementar mecanismos de controle de acesso nos roteadores. Essas tecnologias evoluíram gradativamente, até atingirem um nível muito grande de complexidade e sofisticação. No começo, a função de firewall era atribuída a vários componentes, que ficavam responsáveis por efetuar o controle de acesso entre duas redes com níveis de confiança distintos – por exemplo, entre a internet e uma rede interna. Com o tempo, os fabricantes começaram a fornecer soluções encaixotadas num único software.

Quadro 20 – Gerações de firewall

Geração	Função
1ª geração: filtro de pacotes	Restrição do tráfego com base no endereço IP de origem ou destino
	Restrição do tráfego através da porta do serviço (TCP ou UDP)
2ª geração: filtro de estado de sessão	Regras da 1ª geração
	Restrição do tráfego para o início da conexão (new)
	Restrição do tráfego de pacotes que não tenham sido iniciados a partir de rede protegida (established)
	Restrição do tráfego de pacotes que não tenham número de sequência correto
3ª geração: gateway de aplicativo	Regras da 1ª e da 2ª geração
	Restrição do acesso FTP a usuários anônimos
	Restrição do acesso HTTP a portais de entretenimento
	Restrição do acesso a protocolos desconhecidos na porta 443 (HTTPs)
4ª geração: subsequentes	Solução comercial para redes de comunicação TCP/IP
	Filtro de pacotes dinâmico (stateful inspection)

O firewall isolado não consegue inibir todos os acessos indevidos, mas unido a outras ferramentas de controle pode evitar a entrada de vírus na rede e até detectar uma tentativa de invasão.

Uma desvantagem do firewall é o fato de que, por ser o único ponto de acesso, pode tornar o acesso a outra rede lento. Para resolver isso, uma alternativa é aumentar a capacidade de processamento do firewall empregando soluções de redundância, o que, no entanto, é muito caro.

"O tráfego de informações entre os computadores ou redes e o mundo exterior é examinado e bloqueado quando uma informação não atende a critérios predefinidos de segurança" (BEAL, 2005, p. 94). A função do firewall é analisar pacotes que passam por ele e compará-los a um conjunto de regras a fim de saber que decisão tomar. Algumas tecnologias contribuem para o emprego do firewall numa rede.

A tecnologia de filtro de pacotes funciona com o uso de listas de controle previamente configuradas, as ACLs. Os filtros de pacotes são roteadores que recebem essas listas, e as ACLs são regras que permitem a tomada de ação com base em critérios coletados nos pacotes.

As vantagens do uso de filtro de pacotes residem na velocidade com que os pacotes são analisados, no custo de implantação razoavelmente baixo e na transparência do processo e da manutenção.

Apesar dessas vantagens, o filtro de pacotes também tem sérias limitações de segurança. Ele apresenta problemas em barrar efetivamente um ataque de fragmentação.

Observação

Ataque de fragmentação é uma maneira de fazer com que serviços TCP de máquinas protegidas por um filtro de pacotes sejam acessados mesmo que o filtro não o permita.

Outra tecnologia muito utilizada são os proxies. Criados para resolver os problemas dos filtros de pacotes, os proxies são dispositivos que intermedeiam a conexão entre clientes e servidores, impedindo a comunicação direta entre eles.

O filtro de pacotes dinâmico (stateful inspection), em vez de trabalhar com um conjunto de critérios estáticos, como os utilizados nas ACLs dos roteadores, coleta informações sobre os pacotes trafegados e as armazena num componente denominado **tabela de estados**. Os filtros dinâmicos são a tecnologia mais utilizada em soluções comerciais de mercado. Contudo, eles também usam proxies como auxílio.

Mesmo com as ferramentas mencionadas, muitos sites que empregam firewalls são invadidos por crackers. Isso não quer dizer que esses dispositivos sejam inerentemente falhos, mas a implementação humana às vezes o é. Os principais culpados por invasões em redes são os administradores de firewall que não implementam as regras de forma adequada.

Além disso, como enfatiza Moraes (2010), o firewall controla apenas o tráfego da rede que passa por ele. Assim, em ataques originados no interior da rede, como o tráfego não passa pelo firewall, ele não pode garantir a proteção.

A figura a seguir exemplifica um usuário burlando a proteção do firewall, acessando diretamente a internet por meio de um modem conectado a sua máquina, como um 3G.

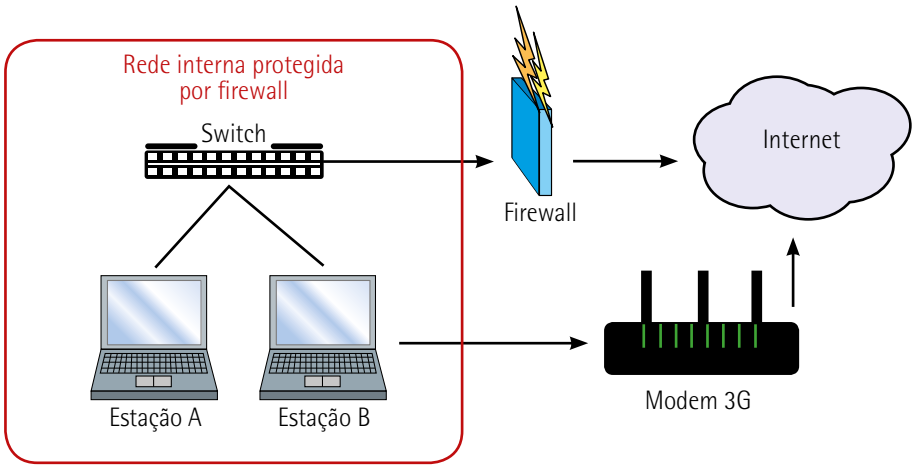

Figura 19 – Usuário da rede interna burlando o sistema de firewall

Existem ainda ataques que o firewall isoladamente não consegue evitar, como ataques de Back Orifice, alguns tipos de DoS, autenticações fraudulentas, backdoors e falhas humanas.

Observação

Back Orifice ("orifício traseiro", em inglês) é uma ferramenta de administração remota, para sistemas operacionais da Microsoft, muito utilizada em fraudes bancárias. O nome é uma brincadeira com o Back Office da Microsoft.

De acordo com Moraes (2010, p. 166), o proxy

> [...] é um servidor que literalmente faz a intermediação da comunicação de um equipamento na rede segura com um equipamento na rede externa. Vamos imaginar que um computador A deseja se comunicar com um computador B. Todas as conexões devem ser estabelecidas pelo proxy. Assim, o computador realiza uma conexão com o proxy, que estabelece uma conexão com o computador externo à rede (B), sendo o proxy responsável pela monitoração e pelo controle do tráfego.

Quadro 21 – Vantagens e desvantagens no uso de proxies

Vantagens	Desvantagens
Redes totalmente isoladas umas das outras	São mais lentos e menos flexíveis
Recursos de log (registro)	Podem exigir configuração dos clientes
Recursos de cache	Precisam ser atualizados para cada novo serviço (ou aplicação) criado e inserido na rede
Balanceamento de carga	

Adaptado de: Moraes (2010, p. 166).

Com a implantação do proxy, 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, caso em que não existe nenhum tipo de configuração das máquinas clientes, ou não transparentes, o que exige configuração.

Na figura a seguir, a máquina interna inicia uma conexão usando 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 de destino. O proxy usa o endereço IP externo próprio como origem e cria seu próprio número de sequência.

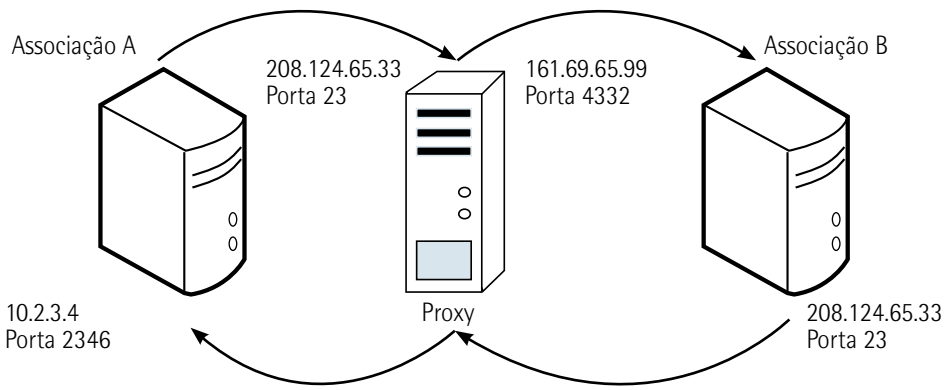

Figura 20 – Funcionamento do proxy

O reply da máquina remota é enviado para o proxy. Este, por sua vez, casa a resposta com a requisição inicial da máquina interna e remonta o pacote enviado com o endereço da máquina interna como destino, o endereço de origem da máquina remota e a porta remota.

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

Existem proxies que trabalham apenas em 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 só podem ser executadas por ele, que tem a função de separar a rede interna da externa.

Os proxies de aplicação manipulam dados complexos das camadas de aplicação, detectando tentativas de quebra da segurança. Devido a essa funcionalidade, são mais lentos que firewalls baseados em filtro de pacotes. Em razão da interatividade com as aplicações, esses proxies não estão disponíveis para alguns tipos de serviço de aplicações específicas.

A configuração da política de segurança num firewall baseado em proxy deve seguir alguns passos lógicos para sua efetiva atuação:

- Determine os tipos de proxy usados no firewall.
- Liste as máquinas internas que podem usar o proxy.
- Ajuste os requerimentos de permissão ou negação a determinados destinos e os requisitos de autenticação.

Para definir o padrão, são necessárias as seguintes permissões:

- **Da rede interna**: permitir FTP, Telnet, NNTP (network news transfer protocol), 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 empregado para determinar a política aplicável. Algumas regras podem ser usadas para grupos de máquinas, criando políticas de segurança gerais.

Os principais tipos de proxy são:

- **De aplicação**: WWW, FTP, Telnet, Mail, NNTP, SQL (structured query language) etc.
- **De circuito**: estão em nível de rede (endereços IP e portas TCP/UDP).
- **Reversos**: trabalham de forma reversa, permitindo o acesso a recursos internos.
- **De cache**: retêm os sites mais usados para reúso, sem a necessidade do acesso direto à internet.

Quadro 22 – Comparativo entre ferramentas utilizadas com firewalls

Ferramenta	Autenticação	Autorização	Auditoria
Filtro de pacotes simples	Não	Sim, apenas para endereços IP	Não
Filtro de pacotes stateful	Não	Sim	Limitada
Proxy de circuito	Não	Sim	Limitada
Proxy de aplicação	Sim	Sim, para endereços IP e ID de usuários	Sim

Adaptado de: Moraes (2010, p. 169).

O firewall proxy e filtro tem uma arquitetura que 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 em serviços inseguros, que necessitem do nível de segurança de um proxy.

A figura a seguir mostra um firewall baseado em proxy. É importante observar que as estações da rede devem ter a configuração do browser a fim de apontar para o proxy. Nesse caso, é preciso configurar 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.

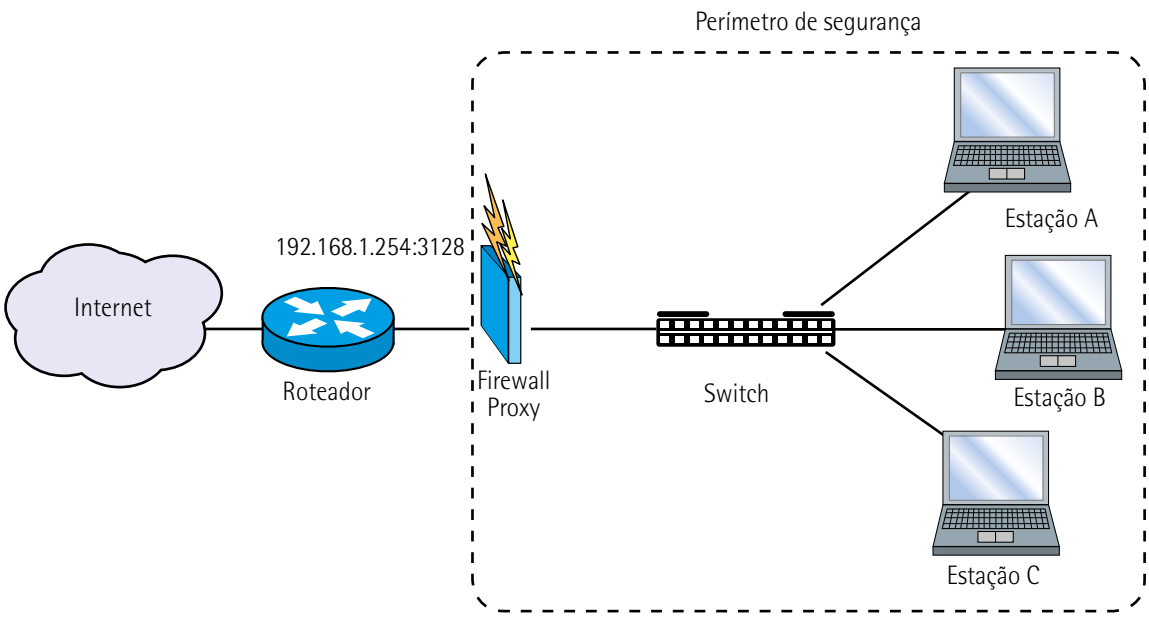

Figura 21 – Arquitetura de firewall proxy

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

- gateway de VPN;
- análise de conteúdo (content screening);
- tradução de endereços de rede (NAT);

- autenticação de usuários;
- balanceamento de carga (load balancing).

Lembrete

Atenção ao configurar o sistema de firewall. Cerca de 90% das falhas de segurança nos firewalls estão associadas à má configuração.

Um firewall pode ser usado ainda para bloquear determinadas URLs, como de sites de pornografia, piadas, jogos ou qualquer outro conteúdo que não faça parte da política de segurança da empresa. Listas de sites proibidos podem ser inseridas no firewall manualmente, a partir de regras, ou dinamicamente, por meio de um software que se agrega à solução de firewall e que recebe diariamente a lista com os sites não permitidos.

Além de executar as funções de controle do acesso e do tráfego, o firewall funciona como um gateway de VPN, realizando conexões criptografadas e tuneladas através de protocolos como o IPSec (internet protocol security), que implementa algoritmos criptográficos como AES (advanced encryption standard) e 3DES.

5.3 Bastion host

Os bastion hosts são estações de trabalho colocadas fora da rede interna, mas dentro da rede perimetral, que visam reforçar a segurança da máquina que é acessada pela internet, pois, se ela não for comprometida e o firewall estiver configurado corretamente para bloquear os acessos através dela, não sobrarão muitas opções para o intruso. É necessário que os equipamentos colocados nessa posição não tenham vulnerabilidades.

Essas máquinas costumam ter sua segurança fortificada, num processo chamado de **hardening**, o qual envolve tarefas como garantir que serviços desnecessários sejam desabilitados. No entanto, não se pode confiar unicamente no processo de hardening, pois mesmo com ele ainda existe a possibilidade de a máquina ter sua segurança comprometida.

Por causa disso, os bastion hosts costumam ser isolados em segmentos de rede específicos, numa tentativa de dificultar a propagação de ataques que os utilizem como plataformas.

5.4 Perímetro de segurança

O perímetro de segurança significa uma faixa de delimitação territorial. Num prédio, costumamos ter um perímetro físico da calçada ao começo da construção, o qual o separa da rua. Internamente, podemos ter diversos outros perímetros, sempre representando um espaço físico que se interpõe entre zonas com níveis de proteção diferentes.

Os perímetros são um conceito bastante importante para a segurança física e podem, de maneira muito semelhante, ser transpostos para a segurança em redes. Frequentemente, perímetros são usados para separar redes internas da internet ou de redes que se conectem a fornecedores, com o objetivo de proteger as primeiras. A maioria das estratégias de proteção baseia-se na criação e na construção dos perímetros de acordo com o nível de confiança das conexões, considerando-se a importância dos ativos a proteger.

> O uso do conceito de perímetros em estratégias de segurança em rede leva a desenhos em que uma rede intermediária é criada e interposta entre outras duas que tenham níveis de confiança diferentes. A divisão entre internet e rede interna já citada seria o melhor exemplo. Esses segmentos intermediários recebem o nome de rede perimetral (RAMOS, 2008, p. 164).

Uma aplicação específica de redes perimetrais é conhecida como DMZ (demilitarized zone) e consiste numa rede perimetral que concentra máquinas acessadas externamente. Ela é colocada entre a rede da qual os acessos externos são originados, em geral a internet, e a rede que gostaríamos de proteger contra esses acessos, comumente a rede interna.

O desenho se completa por um firewall conectando a rede externa à DMZ e outro ligando essa última à rede interna. Sempre que máquinas são acessadas por clientes externos vindos de um ambiente não confiável, deve-se considerar a hipótese de invasão ou comprometimento da segurança. Se uma máquina é invadida e está situada na rede interna, em vez de na DMZ, automaticamente o invasor é capaz de, a partir dessa máquina, disparar ataques para outros recursos.

A ideia de colocar máquinas acessadas externamente num segmento isolado e intermediário faz com que, mesmo em caso de invasão, o invasor tenha um mecanismo de segurança entre ele e a rede mais crítica em termos de proteção. Esse mecanismo, como já mencionado, é um firewall que filtra os pacotes e implementa regras rígidas de controle de acesso. Além disso, essas máquinas costumam ser bastion hosts, ou seja, passaram por um processo de hardening.

Lembrete

O processo de hardening consiste em configurar um equipamento instalando nele todas as ferramentas de segurança necessárias para enfrentar um ataque.

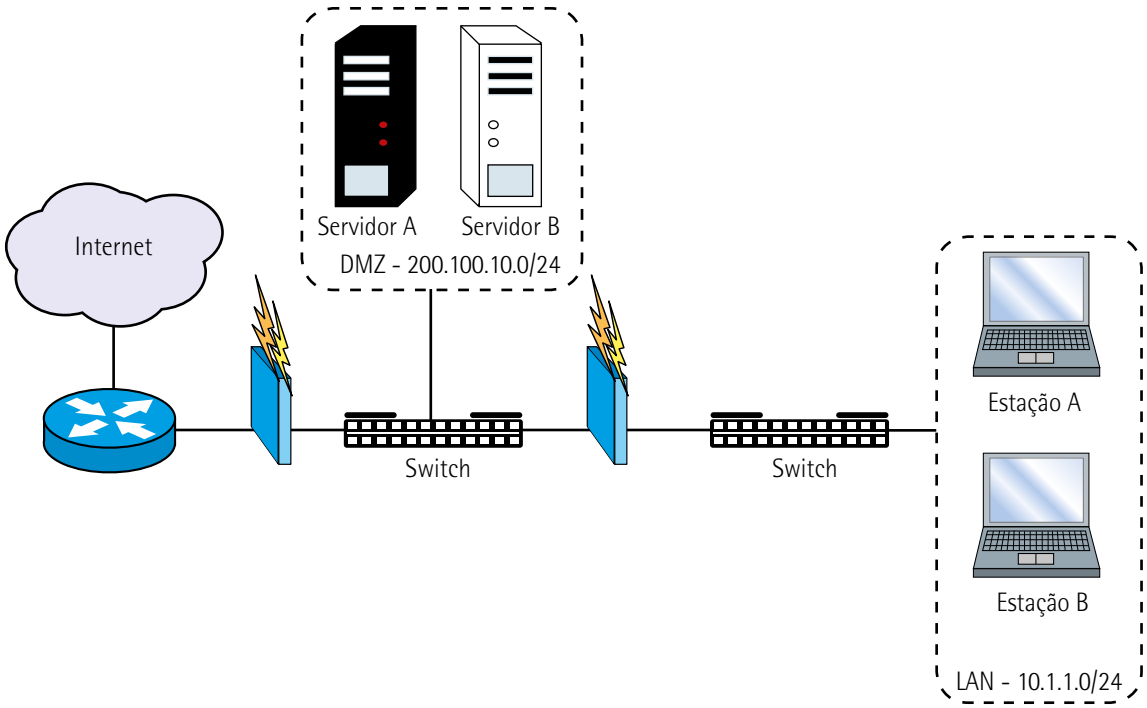

Figura 22 – Topologia de uma rede DMZ

As DMZs, em seu significado original, são faixas territoriais monitoradas, nas quais o uso de equipamentos militares é proibido. Um exemplo atual de DMZ é a faixa que existe entre a Índia e o Paquistão. Em caso de tentativa de invasão por parte da Índia, o exército desse país teria necessariamente de cruzar essa extensão territorial, o que permitiria detectar a ação com antecedência e daria ao Paquistão um tempo precioso para responder ao ataque.

As DMZs criadas para as redes têm a mesma finalidade. Se uma máquina nessa rede perimetral tiver sua segurança comprometida, a equipe de segurança terá tempo para detectar o incidente e responder de forma apropriada, antes que o ataque atinja os ativos internos, nos quais reside o maior esforço em termos de proteção. Por isso, é muito comum que as máquinas da DMZ sejam monitoradas de perto, seja de maneira automática, com IDSs, seja de forma manual.

Para aumentar ainda mais a segurança e garantir a defesa em profundidade, costuma-se combinar a segurança fornecida por um firewall ou um IPS com a chamada **segurança em host**, transformando as máquinas que recebem acesso externo em bastion hosts.

Toda vez que uma rede tem a sua frente um dispositivo de controle de acesso, como um firewall ou um IPS, ela é chamada de **screened subnet** ("rede filtrada", em inglês). Existem variações do conceito de DMZ nas quais, em vez de utilizar dois firewalls, criando uma rede perimetral no meio deles, apenas um dispositivo é usado, conectando diversas redes, todas elas filtradas. É uma tentativa de simular a mesma proteção, porém consumindo menos recursos.

5.5 Sistemas de detecção, prevenção e reação

Moraes (2010) afirma que, para garantir a segurança de uma rede, é necessário pensar em três elementos:

- **Sistemas de detecção**: IDS, scanning por antivírus, auditoria etc.
- **Sistemas de prevenção**: IPS, firewall, encriptação, autorização etc.
- **Sistemas de reação**: políticas, procedimentos, resposta automática etc.

Os sistemas de detecção de intrusão suplementam a proteção quando existe a necessidade de deixar alguma porta em aberto nos firewalls – por exemplo, quando há troca de informação entre uma aplicação externa e uma interna.

Muitas empresas se preocupam muito em fechar as portas com um firewall, pois assim se sentem seguras, e acabam deixando de lado o investimento em sistemas de detecção de intrusão. No entanto, como visto, um firewall não tem mecanismos de controle de ataques provenientes de dentro da rede, pois ali o tráfego não passa por ele. Para esses casos, a detecção de intrusão é extremamente eficiente. Ela sinaliza ao administrador da rede a existência de uma tentativa de ataque nos servidores e derruba a conexão do invasor.

Os sistemas de detecção de intrusão ou IDSs automatizam essas tarefas pela coleta de informações na rede ou dentro de hosts, analisando-as por meio de uma série de métodos em busca de padrões que caracterizem ataques.

Os sistemas de detecção de intrusão utilizam os seguintes métodos:

- **Análise de assinatura de ataque**: o sistema já traz armazenados os principais ataques realizados por hackers. Ele simplesmente monitora o comportamento dos servidores para verificar a ocorrência do ataque. Se o cracker utilizar um ataque novo, do qual o sistema não tem a assinatura, ele não será reconhecido.
- **Análise de protocolo**: o sistema verifica constantemente os protocolos de aplicação para determinar se existe algo errado. Um ataque de DNS (domain name system) do tipo overflow do buffer do bind, por exemplo, pode ser detectado pela análise de protocolo, pois esses ataques incluem alguns bytes no pacote que são identificáveis.
- **Detecção de anomalia**: o método mais complexo de detecção de intrusão. Envolve o monitoramento de CPU, logs do sistema operacional, memória e discos dos servidores para verificar se está ocorrendo alguma anomalia no servidor. Há anomalias que podem ser detectadas em aplicações, como a realização de uma query DNS num servidor web que a princípio não deveria ter o DNS rodando.

Muitas pessoas acreditam que os sistemas de detecção de intrusão identificam mau uso da rede ou ataques. Na verdade, eles identificam anomalias. É função do administrador de rede determinar

se essas anomalias correspondem a ataques. Os falsos positivos são o grande problema dos sistemas de detecção de intrusão. No entanto, sistemas de última geração eliminam drasticamente o número de falsos positivos.

Quando um processo é identificado, prioridades devem ser definidas. Como esses sistemas trabalham 24 horas por dia, é preciso haver administradores de rede de plantão, que possam ser acionados quando ataques forem rastreados.

Quadro 23 – Tipos de sistema de detecção de intrusão

Tipo	Função
Sistema baseado na rede	Trabalha com a análise de pacotes da rede
Sistema baseado nas estações	Coleta logs e eventos do sistema operacional das estações
Sistema baseado na integridade de arquivos	Verifica a integridade dos arquivos utilizando sistemas antivírus e auditoria

Adaptado de: Moraes (2010, p. 194).

Existem ainda sistemas híbridos, baseados na rede e nas estações. Já os sistemas baseados na integridade de arquivos criam um hash criptografado dos arquivos mais importantes do sistema e alertam quando ocorre alguma mudança neles.

As principais características de um sistema de detecção de intrusão são:

- **Execução contínua**: independentemente do horário comercial da empresa, o sistema de detecção precisa funcionar as 24 horas do dia, como o servidor.
- **Não tolerância a falhas**: falhas nesse sistema podem facilitar a ocorrência de um ataque.
- **Mínimo overhead na rede**: em razão de suas características de scanning contínuo da rede, deve trabalhar com baixo overhead, a fim de não prejudicar o tráfego normal de dados.
- **Dificuldade de ser atacado**: deve ser um sistema pouco vulnerável a ataques.

Qualquer ação a ser tomada por um IDS precisa ser dirigida a um dispositivo externo, como um firewall. O IDS pode enviar um TCP reset ou um ICMP unreachable, ou mesmo configurar uma ACL de bloqueio no firewall.

Quadro 24 – Componentes de um IDS

Componente	Descrição
Agente	Peça de software responsável pela coleta de dados. No caso de sistemas network-based, esse componente roda normalmente num equipamento separado, conectado ao segmento de rede monitorado.
Coletor de eventos	Componente que recebe os dados dos diferentes agentes que integram o IDS, centralizando o recebimento.

Base de dados	Banco de dados de alta performance, que reúne as informações enviadas pelos agentes e recebidas pelo coletor de eventos.
Gerenciador central	Principal componente de controle do IDS. Muitas vezes, é dentro dele que se encontra o mecanismo de análise das informações, responsável por interpretar os dados e detectar a incidência de incidentes.
Sistema de alerta	Elemento responsável pela interface com aqueles que necessitem enviar avisos a respeito de ataques. Pode gerar alertas de diversos tipos.
Interface gráfica	Alguns sistemas, em especial as soluções comerciais, fornecem uma interface gráfica que permite gerenciar e monitorar os sistemas. Essa interface pode ser um componente isolado, que se conecta ao gerenciador central, ou então fazer parte desse último.

Uma vez conhecidas as tecnologias disponíveis para a construção de um IDS, a fim de implementá-lo corretamente, devem-se examinar os fatores externos que influenciarão o projeto.

Primeiro, é preciso fazer um levantamento dos requisitos, o que consiste, basicamente, num mapeamento das necessidades do sistema, a fim de permitir a escolha das opções mais adequadas. Dois tipos de requisito devem ser analisados: técnicos e organizacionais.

No que diz respeito aos requisitos técnicos, o ambiente que será monitorado tem de ser estudado e compreendido. Isso envolve um conhecimento sobre a topologia, os serviços fornecidos pela rede e os usuários que os acessam. Inclui-se aqui o desenho das proteções existentes (firewalls, por exemplo).

É necessário traçar de forma clara os principais objetivos a atingir com o uso do IDS: os ataques que mais preocupam vêm de dentro ou de fora? As informações produzidas pelo IDS serão utilizadas de que forma? O monitoramento será feito pela equipe de segurança ou por uma equipe de monitoramento de rede?

É possível que os requisitos técnicos sejam afetados pela política de segurança da organização. Entre outras coisas, esse documento pode conter especificações sobre tecnologias, responsabilidades, procedimentos de resposta a incidentes e práticas de investigação.

Os requisitos organizacionais, por sua vez, envolvem tanto necessidades internas à organização quanto demandas externas a ela (obrigações legais, por exemplo). Esses elementos devem ser avaliados para garantir o projeto de uma solução em conformidade com os objetivos organizacionais.

Além dos requisitos, é preciso considerar as limitações que podem causar impacto no projeto do IDS. As duas mais importantes são: orçamento e pessoal. Soluções comerciais tendem a ser mais caras, porém mais fáceis de gerenciar, e servem bem para ambientes com disponibilidade de recurso financeiro e falta de pessoal. Ambientes com baixo orçamento, mas com pessoal capacitado disponível, podem se valer dessa vantagem e reunir a equipe para montar excelentes soluções usando software livre. A situação mais comum, no entanto, é que, em maior ou menor grau, ambas as limitações existam, forçando a busca de soluções de software livre ou soluções comerciais econômicas e simples de administrar. Há diversas opções gratuitas, mas deve-se ter em mente que o trabalho associado a sua continuidade costuma ser sempre um pouco maior do que o de soluções comerciais.

De acordo com Moraes (2010, p. 195), os sistemas de prevenção de intrusão ou IPSs

> [...] permitem, além de alertar uma tentativa de ataque, realizar o seu bloqueio. Esses equipamentos normalmente estão conectados aos segmentos críticos da rede, em linha, ou seja, todo o tráfego a ser inspecionado precisa passar por eles. Eles permitem a detecção e o bloqueio automático de ataques.

Em geral, esse tipo de equipamento trabalha na camada de enlace do modelo OSI (open system interconnection), a camada 2, e não é necessário nenhum tipo de reconfiguração da rede para ele ser instalado.

Os IPSs realizam uma inspeção muito profunda no pacote, que vai até a camada de aplicação do modelo OSI (camada 7). Um IPS permite detectar as seguintes ameaças à rede (inclusive à rede sem fio): propagação de vírus, propagação de worms, ataques direcionados a sistemas operacionais, ataques direcionados à aplicação web – como cross-site scripting, injeção de PHP (hypertext preprocessor) e injeção de SQL–, exploração de vulnerabilidades das principais aplicações, spam, phishing, spyware e uso da rede por aplicações não permitidas, como P2P (peer to peer).

Esses equipamentos costumam ter alta capacidade de processamento, trabalham com interfaces gigabit ethernet ou 10 gigabit ethernet e realizam a inspeção em arquiteturas de processamento distribuído com microprocessadores dedicados Asics (application specific integrated circuits) e FPGAs (field-programmable gate arrays).

Os IPSs têm baixas taxas de falsos positivos e permitem detectar ainda ataques de negação de serviço.

Alguns benefícios de adotar uma solução de IPS:

- **Redução das chamadas de help desk**: uma vez que o IPS realiza o bloqueio das ameaças e protege os dispositivos, em especial o computador dos usuários, diminui a necessidade de ação da equipe de suporte.

- **Aumento do conhecimento e da visibilidade do tráfego da rede**: o IPS permite monitorar tráfegos e fluxos e identificar comportamentos anômalos. Ele atua como um espião e detecta tráfegos não esperados e não autorizados – por exemplo, ataque interno, ataque de DoS e uso de aplicações não autorizadas (como P2P). Previne a perda de dados por meio de filtros de DLP (data loss prevention).

- **Controle de banda**: um dos principais recursos do IPS é monitorar o uso de banda pelas aplicações e empregar limitadores de banda (rate limit). Esse recurso é essencial para o controle da rede. Vários clientes o utilizam para evitar o congestionamento causado por streaming de vídeo e acesso a redes P2P. Em determinado caso, o IPS comprovou o uso de mais de 40% do link de comunicação com tráfego não permitido (P2P), o que aumentava os custos associados e gerava lentidão nas aplicações válidas e essenciais à rede.

- **Serviço de reputação**: permite bloquear uma ameaça sem a necessidade de inspecionar os pacotes. Isso é possível porque já existem na internet serviços que monitoram as ações e

identificam propagação de worms, servidores de botnets, servidores que hospedam sites de phishing, origens de ataques de DoS, redes P2P e sites com tráfego malicioso. De posse desses endereços, realiza-se um ranking da ameaça na base de dados de reputação. Isso permite que o usuário, por política, bloqueie as ameaças de acordo com nível de criticidade (de 0 a 10), tipo de ameaça (spyware, worm, phishing, botnet etc.) ou mesmo país de origem. Essa base de dados de reputação é atualizada a cada duas horas.

- **Redução dos custos com a recuperação de máquinas**: sempre dizemos que prevenir é mais barato que remediar. Ataques bem-sucedidos numa rede trazem prejuízos imensos à organização, além de causar a indisponibilidade das máquinas, uma vez que elas ficam fora de operação até serem reinstaladas. O grande problema é a perda ou o roubo dos dados da máquina comprometida, um prejuízo às vezes incalculável. O rebuild de máquinas pode levar mais de duas horas por computador.

- **Aumento da produtividade**: o tempo para recuperar computadores comprometidos pode ser muito grande, e trabalhos salvos, mas que não tinham backup, podem simplesmente se perder quando a máquina é comprometida. O IPS, por proteger contra esse tipo de ação, contribui para o aumento da produtividade. Ele reduz em 99% a quantidade de incidentes de segurança na rede.

- **Combate a outbreaks**: a cada ano surge uma ameaça crítica, um outbreak, que gera grandes problemas e indisponibilidade nas redes corporativas. O grande último outbreak foi o Conficker, um worm que se propagava rapidamente pela rede, derrubando o serviço de DNS interno e congestionando o serviço de autenticação do Windows (Active Directory). Usuários que acreditaram que o antivírus e o firewall fossem capazes de bloquear essa ameaça foram surpreendidos pela parada total da rede. Alguns outbreaks são capazes de infectar toda a rede em poucos minutos.

- **Função de patch virtual**: normalmente, perde-se muito tempo para atualizar todo o parque de máquinas quando uma nova ameaça é identificada. A gerência de TI costuma realizar as atualizações em fins de semana, o que, às vezes, pode ser tarde demais. Um IPS instalado na rede, porém, atua como um patch virtual. Assim, mesmo que as máquinas estejam vulneráveis, qualquer tentativa de explorar esse cenário será bloqueada, protegendo as estações.

- **Função de web application firewall**: é notória a dificuldade em alterar uma aplicação para que ela se torne menos vulnerável. É muito mais barato bloquear ameaças pela rede do que realizar correções na aplicação. Nesse ponto, o IPS é um instrumento fundamental para proteger as aplicações, especialmente as aplicações web.

- **Proteção da infraestrutura de voz sobre IP**: as reduções de custo atreladas ao uso de voz sobre IP são uma realidade no ambiente de TI de uma organização moderna. Entretanto, esse ambiente é vulnerável a uma série de ataques, os quais procuram indisponibilizar o serviço ou permitir a realização de chamadas não autorizadas. O IPS tem uma cobertura completa de vacinas que protegem contra ataques à infraestrutura VoIP (voice over internet protocol).

- **Proteção do firewall**: o IPS complementa a ação do firewall no estabelecimento da política de segurança. Entretanto, vale ressaltar que o próprio firewall pode estar suscetível a um ataque,

especialmente de negação de serviço. Logo, pode-se fazer uso de um IPS para proteger, além de toda a infraestrutura de máquinas e servidores, os serviços de firewall.

- **Ação de quarentena**: caso seja identificada uma fonte de ataques na rede interna, o IPS permite adotar uma ação de quarentena, que consiste em isolar a máquina comprometida para que ela não dissemine a ameaça pela rede.

Como vimos antes, existem muitos softwares maliciosos (vírus, worms, cavalos de Troia etc.). A introdução de um dispositivo infectado numa estação da rede ou a instalação de softwares não confiáveis podem colocar em risco a segurança da informação.

Por isso, são necessárias medidas de proteção, como políticas de segurança, programas de conscientização dos usuários, procedimentos controlados para a importação de arquivos e softwares, instalação e atualização regular de softwares antivírus e exame periódico de computadores e mídias.

A segurança de sistemas aplicativos demanda controles que estejam de acordo com os requisitos de segurança existentes: validação dos dados de entrada, controle do processamento interno, validação da saída e controle da transmissão de mensagens.

Também é necessário proteger as informações no ambiente do usuário final. Para isso, devem-se implantar medidas de controle do usuário dentro do ambiente lógico. Considere as indicações do quadro a seguir.

Quadro 25 – Proteções aplicáveis ao usuário final

Controle	Prescrição
Proteção das informações críticas	Adote mecanismos para proteger as informações críticas que precisam ser compartilhadas. O uso de criptografia é recomendado.
Atualização dos softwares antivírus	Atualize constantemente a lista de vírus conhecidos.
Uso de firewall	Use um firewall não apenas na rede, mas também nas estações de trabalho individuais.
Procedimentos de logon	Limite o tempo máximo para a entrada no sistema e o número máximo de tentativas de entrada.
Políticas e controles	Estabeleça regras para o uso de equipamentos portáteis, como notebooks e celulares.

Resumo

Assim como as técnicas de invasão, os dispositivos destinados à segurança em redes também evoluem. Nesta unidade, pudemos observar em detalhes esses dispositivos, sua estrutura e os benefícios que a implantação, a configuração e a manutenção eficiente deles podem trazer aos administradores de rede. Elementos como roteador de borda, firewall, proxy, bastion host e perímetro de segurança são ótimos aliados na proteção de dados.

Vimos também os sistemas de detecção, prevenção e reação. No âmbito da detecção, consideramos os sistemas de detecção de intrusão, que automatizam as tarefas por meio da coleta de informações na rede ou dentro de hosts, analisando-as mediante uma série de métodos em busca de padrões que caracterizem ataques.

Com relação à prevenção, destacamos os sistemas de prevenção de intrusão, que, além de alertar sobre uma tentativa de ataque, ainda podem bloqueá-la. Entre as ameaças que esses sistemas previnem, encontram-se a propagação de vírus e worms, a exploração de vulnerabilidades das principais aplicações e o uso da rede por aplicações não permitidas.

Quanto à reação, associa-se à implementação de políticas de segurança, programas de conscientização dos usuários, procedimentos controlados para a importação de arquivos e softwares, instalação e atualização regular de softwares antivírus e exame periódico de computadores e mídias.