



RESUMO TÉCNICO

Segurança de Rede:

Um guia
simples
para
firewalls

Segurança de Rede

Guia simples para firewalls

A perda de dados insubstituíveis é uma ameaça bastante real para qualquer proprietário de empresa cuja rede está conectada ao mundo exterior. O acesso remoto para funcionários e a conexão à Internet podem melhorar muito a comunicação. O acesso à Internet abre os horizontes para a comunicação com clientes e fornecedores e é uma inesgotável fonte de informações. Contudo, essas mesmas oportunidades expõem a LAN à possibilidade de sofrer ataques de hackers e de ser utilizada inadequadamente pelos próprios funcionários da empresa.

Algumas considerações devem ser feitas antes de você decidir o nível correto de segurança de que sua rede precisa. O primeiro aspecto a ser considerado é o quanto valem seus dados. Uma resposta rápida seria: "Talvez muito mais do que você imagina". Ao pensar no valor de seus dados, lembre-se de riscos como responsabilidade legal e perda da vantagem competitiva ou o efeito da perda de produção se sua rede for comprometida. A maioria dos analistas diz bem claramente: "Se você está conectado à Internet, precisa de um firewall".

Os benefícios de uma conexão com a Internet são claros. Este artigo aborda os riscos que você corre quando se conecta à Internet, descreve os tipos de ataques que podem ocorrer e oferece uma visão geral da tecnologia de firewall, que pode proteger sua rede de hackers. Mais especificamente, discutimos a implementação de um firewall e o que você deve levar em consideração ao escolher o tipo de firewall de que precisa.

Por que Instalar um Firewall – Estou Realmente Correndo Algum Risco?

Qualquer pessoa pode se tornar um hacker. Não é preciso ser um jovem com grandes conhecimentos de tecnologia para causar um enorme estrago em uma rede. Inúmeras ferramentas e utilitários podem ser facilmente baixados da Internet e, com a ajuda deles, praticamente qualquer pessoa pode se

tornar um competente hacker ao simples toque de um botão.

Há especialistas que dizem: "Se você está conectado à Internet, precisa de um firewall". A decisão talvez não envolva maiores complicações. No entanto, você provavelmente irá considerar uma série de fatores. Comece com as perguntas básicas que você faria sobre qualquer outro sistema de segurança.

Tenho alguma coisa que vale a pena proteger?

Lembre-se de considerar:

- Informações confidenciais sobre clientes, fornecedores ou funcionários que poderiam expô-lo a um processo, caso você permitisse que alguém mais tivesse acesso a elas
- Propriedade intelectual que lhe proporciona vantagem competitiva no mercado
- Relatórios cruciais da empresa que teriam de ser recuperados e/ou recriados

Nem sempre é seguro supor que ninguém mais está interessado em seus dados. Alguns hackers operam sem ter nenhum ganho em mente. Eles podem capturar seus dados ou corromper seu sistema simplesmente porque são capazes de fazê-lo.

Minhas informações importantes já não estão suficientemente protegidas?

A verdade é que se sua propriedade eletrônica é valiosa, ela pode não estar tão segura quanto você gostaria que estivesse. Você mesmo pode ajudar muito na proteção de seu sistema se:

- Fizer o backup de suas informações no final do expediente
- Criar pastas não compartilhadas com senhas de difícil acesso e regras para essas senhas
- Utilizar seu roteador de acesso ou browser para filtrar o tráfego de entrada proveniente de todos os sites, exceto de sites seguros

Infelizmente, os hackers têm muitas ferramentas sofisticadas à disposição. Se tiver tempo e determinação, um hacker habilidoso pode violar as

ÍNDICE

Por que instalar um firewall – Estou realmente correndo algum risco?	1
O que é um firewall?	2
Tipos de ataques	2
Tecnologias de firewall	3
Funções e recursos adicionais de um firewall	4
A escolha de um firewall	5
Como projetar um firewall para sua rede	6
Conclusão	6

3DES Padrão de criptografia de dados (168 bits)

DMZ Zona desmilitarizada

DoS Serviço negado

FTP Protocolo de transferência de arquivos

HTTP Protocolo de transferência de hipertexto

ICSA Associação Internacional de Segurança de Computadores

LAN LAN

NAT Conversão de endereços de rede

POP3 POP3, versão 3

SMTP SMTP

TCP/IP Protocolo de controle de transmissão/Protocolo de Internet

VPN VPN

WAN WAN

garantias de segurança padrão. Se fizer isso, poderá executar programas de software para violar suas senhas. Se você tiver dados valiosos em sua rede e ela estiver exposta a computadores externos, você provavelmente precisará de um firewall.

O que é um firewall?

O firewall é um sistema que impõe uma política de controle de acesso entre duas redes – como a sua LAN privada e a Internet, que é pública e vulnerável. O firewall determina quais os serviços internos que podem ser acessados externamente e vice-versa. Os meios reais pelos quais isso é feito variam muito, mas em princípio o firewall pode ser considerado um par de mecanismos: um para bloquear o tráfego e outro para permitir o tráfego. Um firewall representa mais do que uma tranca na porta da frente de sua rede – é também seu segurança particular.

Os firewalls também são importantes porque oferecem um único “ponto de restrição” onde a segurança e as auditorias podem ser impostas. Um firewall pode fornecer ao administrador da rede dados sobre o tipo e a quantidade de tráfego que passam por ela, quantas tentativas foram feitas para invadi-la e assim por diante. Assim como um sistema de segurança de circuito fechado de TV, seu firewall não apenas bloqueia o acesso, mas também monitora quem está “bisbilhotando” e auxilia na identificação daqueles que tentam violar a segurança.

Finalidade básica de um firewall

Basicamente, um firewall faz o seguinte para proteger sua rede:

- Bloqueia dados de entrada que possam conter um ataque de hacker
- Oculta informações sobre a rede, fazendo com que pareça que todo o tráfego de saída é proveniente do firewall e não da rede. Isso é denominado NAT (Network Address Translation)
- Filtra o tráfego de saída, a fim de limitar o uso da Internet e/ou acesso a localidades remotas

Níveis de filtragem

Um firewall pode filtrar tanto o tráfego de entrada como de saída. Como o tráfego de entrada representa uma ameaça muito maior à rede, geralmente

é filtrado mais cuidadosamente do que o tráfego de saída.

Ao procurar por produtos de software ou hardware de firewall, você provavelmente ouvirá falar de três tipos de filtragem desempenhados por um firewall:

- Filtragem que bloqueia quaisquer dados de entrada que não tenham sido especificamente solicitados por um usuário da rede
- Filtragem pelo endereço do remetente
- Filtragem pelo conteúdo da comunicação

Imagine os níveis de filtragem como um processo de eliminação. Primeiro o firewall determina se a transmissão de entrada foi solicitada por um usuário da rede, rejeitando as demais. Qualquer tráfego que tem entrada permitida é examinado mais detalhadamente. O firewall verifica o endereço do computador do remetente para se certificar de que seja um site confiável. Ele também verifica o conteúdo da transmissão.

Tipos de Ataques

Antes de determinar com precisão o tipo de firewall de que você precisa, será necessário, antes de mais nada, compreender a natureza das ameaças à segurança existentes. A Internet é uma grande comunidade e, como qualquer outra, é constituída de bons e maus elementos. Os maus elementos variam de estranhos incompetentes que causam danos não-intencionais, a hackers competentes e maldosos, que planejam ataques deliberados a empresas, utilizando a Internet como sua arma preferida.

De modo geral, existem três tipos de ataques que podem prejudicar sua empresa:

- *Roubo de informações*: roubo de informações sigilosas da empresa, como dados sobre registros de funcionários, registros de clientes ou propriedade intelectual da empresa
- *Sabotagem de informações*: alteração de informações, na tentativa de manchar a reputação de uma pessoa ou da empresa, como alteração dos registros médicos ou curriculares de funcionários ou upload de conteúdo pejorativo em seu Web site

- *DoS (Denial of Service ou serviço negado):* tornar indisponível a rede ou os servidores da empresa para que usuários legítimos não possam acessar os serviços ou para que as operações normais da empresa, como a produção, sejam obstruídas.

Tentativas de obter acesso

Um hacker pode tentar obter acesso apenas como diversão ou por ambição. Uma tentativa de obter acesso geralmente começa com a coleta de informações sobre a rede. Os ataques posteriores utilizam essas informações para alcançar o verdadeiro objetivo – apoderar-se de dados ou destruí-los.

O hacker pode utilizar um scanner de portas - um software que pode mapear uma rede. Depois, ele poderá descobrir a estrutura da rede e o software que está sendo executado nela.

Quando o hacker tem uma idéia de como é a rede, ele pode explorar falhas de software conhecidas e utilizar ferramentas para causar danos. É possível apagar arquivos administrativos e apagar unidades, embora uma senha bem elaborada geralmente dificulte essa tarefa.

Felizmente, um bom firewall é imune a varredura de portas. À medida que novos scanners de portas são desenvolvidos para burlar a imunidade, os fabricantes de firewalls produzem correções para preservá-la.

Ataques DoS

Os ataques DoS são feitos por pura má fé. Não resultam em nenhum benefício para o hacker, a não ser o “prazer” de fazer com que toda a rede ou parte dela fique indisponível para usuários autorizados. Os ataques DoS sobrecarregam o sistema para que fique indisponível – eles não permitem que você use seus serviços de rede. Para sobrecarregar o sistema, o hacker envia grandes pacotes de dados ou programas que exigem que o sistema responda continuamente a um comando adulterado.

Para lançar um ataque DoS, o hacker precisa conhecer o endereço IP da máquina-alvo. Um bom firewall não revela seu endereço IP ou os endereços IP da LAN. O hacker pode pensar que conseguiu se conectar à rede quando,

na verdade, se conectou ao firewall – e não é possível travar a rede a partir desse ponto. Além disso, quando o hacker lança um ataque, alguns firewalls conseguem identificar os dados de entrada como um ataque, rejeitá-los, alertar o administrador do sistema e enviar os dados de volta ao remetente, que poderá ser detido.

Tecnologias de firewall

Há firewalls de todos os tipos, tamanhos e preços. A escolha do firewall correto vai depender principalmente das necessidades da sua empresa e do tamanho da sua rede. Esta seção aborda os diferentes tipos de tecnologias de firewall e os formatos disponíveis no mercado.

Acima de tudo, independentemente do tipo ou das funções do firewall escolhido, você deve certificar-se de que ele seja seguro e certificado por uma empresa idônea, como a ICSA (International Computer Security Association). A ICSA classifica os firewalls em três categorias: firewalls de filtragem de pacotes, servidores proxy de aplicativos e firewalls SPI (stateful packet inspection).

Firewall de filtragem de pacotes

Todos os computadores de uma rede têm um endereço geralmente chamado de endereço IP. Um firewall de filtragem de pacotes verifica o endereço do tráfego de entrada e descarta quaisquer endereços que não constem da relação de endereços confiáveis. O firewall de filtragem de pacotes utiliza regras para negar o acesso, de acordo com as informações contidas em cada pacote, como número de portas TCP/IP, endereço IP da fonte/destino ou tipos de dados. As restrições podem ser tão rigorosas ou flexíveis quanto você desejar.

Um roteador de rede pode ter condições de filtrar o tráfego por endereço, mas os hackers têm um pequeno truque, denominado spoofing de IP de origem, que faz com que os dados pareçam ter vindo de uma fonte confiável, até mesmo de sua própria rede. Infelizmente, os firewalls de filtragem de pacotes são suscetíveis a spoofing de IP e sua configuração é difícil e complicada. Qualquer erro de configuração pode deixá-lo vulnerável a ataques.

Servidor proxy

Os servidores proxy de aplicativos examinam o aplicativo usado para cada pacote IP, individualmente, a fim de verificar sua autenticidade. O tráfego proveniente de cada aplicativo – como HTTP para Web, FTP para transferência de arquivos e SMTP/POP3 para e-mail – normalmente exige a instalação e a configuração de aplicativos proxy diferentes. Muitas vezes, os servidores proxy necessitam de administradores para reconfigurar a rede e seus aplicativos (ex: browsers da Web), e esse processo pode ser muito trabalhoso.

Firewall SPI

Esta é a última geração em tecnologia de firewall. A inspeção de pacotes é considerada por especialistas em Internet a tecnologia de firewall mais avançada e segura, pois o firewall examina todas as partes de um pacote IP para decidir se a solicitação de comunicação será aceita ou negada.

O firewall executa o acompanhamento de todas as solicitações de informações originadas na rede. A seguir, examina cuidadosamente cada comunicação de entrada para verificar se foi solicitada, descartando as que não foram. Os dados solicitados prosseguem para o nível seguinte de filtragem. O software de filtragem determina o estado de cada pacote de dados, daí o nome stateful packet inspection (inspeção de estado de pacote).

Funções e recursos adicionais de um firewall

Além da capacidade do firewall de oferecer segurança, uma ampla gama de recursos e funções adicionais está sendo acrescentada aos produtos de firewall padrão. Estão incluídos suporte a Web e a servidores de e-mail, recurso normalmente chamado de zona desmilitarizada (DMZ), filtragem de conteúdo, suporte a criptografia de VPN e suporte a antivírus.

Firewalls de zona desmilitarizada

Um firewall que oferece proteção DMZ é útil a empresas que convidam os clientes a se conectarem a sua rede a partir de fontes externas, seja através da Internet ou de qualquer outro meio

– por exemplo, uma empresa que tenha um Web site ou venda seus produtos ou serviços pela Internet.

Os fatores decisivos para a escolha de um firewall DMZ seriam o número de usuários externos que acessam informações através da rede e a frequência desses acessos.

O firewall DMZ cria uma área de informações protegida (“desmilitarizada”) na rede. Os usuários externos podem acessar a área protegida, porém não o restante da rede. Isso permite que usuários externos obtenham as informações que você gostaria de lhes transmitir e evita que eles obtenham informações às quais você não gostaria que tivessem acesso.

Filtragem de conteúdo

Um filtro de Web site ou de conteúdo amplia a capacidade do firewall de bloquear o acesso a determinados Web sites. Você pode usar esse recurso adicional para assegurar que os funcionários não acessem determinados conteúdos, como pornografia ou material relativo a preconceitos raciais. Com essa função, é possível definir categorias de materiais indesejáveis e obter um serviço que relaciona milhares de Web sites, incluindo esse tipo de material. Você pode escolher entre bloquear totalmente o acesso a esses sites ou permitir que sejam acessados, mas que o acesso seja registrado. Esse tipo de serviço deve atualizar automática e regularmente a relação dos sites que não devem ser acessados.

Virtual Private Network

As VPNs são redes de dados privadas que fazem uso da infra-estrutura da rede pública, ou seja, da Internet. A finalidade da VPN é oferecer à empresa os mesmos recursos das linhas telefônicas privadas, mas a custos muito mais baixos. A VPN oferece o compartilhamento seguro de recursos públicos para dados, por meio do uso de técnicas de criptografia, assegurando que somente usuários autorizados possam ver a rede de uma empresa privada ou entrar nela.

Atualmente, as empresas estão considerando o uso das VPNs como uma alternativa com ótimo custo-benefício

para conectar com segurança suas filiais, funcionários remotos e principais parceiros/clientes às suas LANs privadas. Hoje, há uma ampla gama de firewalls disponíveis que incluem o recurso de criptografia para VPNs ou oferecem esse recurso como opcional. Isso proporciona à empresa uma alternativa simples e de bom custo-benefício, se comparada à opção por linhas privadas ou acesso remoto via modem.

Ao implementar uma VPN, você deve assegurar-se de que todos os dispositivos suportem o mesmo nível de criptografia e de que ela seja suficientemente segura. Até o momento, o Data Encryption Standard de 168 bits (3DES) representa o nível mais potente de criptografia disponível no mercado, e especialistas em segurança o consideram inviolável. Entretanto, é preciso ter em mente que quanto mais alto o nível de criptografia, maior capacidade de processamento será exigida pelo firewall. Um pequeno número de fabricantes de firewalls está hoje oferecendo aceleração de VPNs via hardware, visando a melhorar o desempenho do tráfego dessas redes.

Proteção antivírus

Todos devem estar atentos à ameaça representada pelos vírus, uma das formas mais perniciosas de invasão. Usuários desprevenidos podem danificar redes inteiras ao fazer, inadvertidamente, o download de material desconhecido, disseminando poderosos vírus na rede. Devido aos vírus de computador, as empresas têm perdido muito capital, pois, na maioria das vezes, os problemas gerados por eles afetam a produtividade e culminam em altos custos de reparo da rede.

Os firewalls não são projetados para remover ou eliminar os vírus, mas podem ajudar a detectá-los, e esse recurso de detecção é parte importante de um plano geral de proteção contra os vírus.

É importante observar que um firewall só tem condições de proteger a rede a partir do dispositivo de WAN ao qual está conectado. Um servidor de acesso remoto ou PC equipado com modem poderia servir como porta traseira de entrada na rede, desviando, assim, do firewall. O mesmo é válido se o funcionário inserir em seu PC um

disquete infectado por vírus. O mais aconselhável é instalar um software antivírus no PC de cada usuário. Mas o firewall pode ajudar na detecção de vírus, se cada usuário de PC tiver instalada e habilitada em seu computador a versão mais recente de um software antivírus, que seria executada antes que o firewall permitisse ao usuário acessar a Internet ou fazer o download de e-mails.

A escolha do firewall

As funções de um firewall podem ser implementadas como software ou como recurso adicional do roteador/gateway. Por outro lado, os dispositivos de firewall dedicados estão se tornando cada vez mais populares, graças principalmente à sua facilidade de uso, melhor performance e custos mais baixos.

Firewalls baseados em roteadores/firmware

Certos roteadores oferecem recursos limitados de firewall, que podem ser ampliados com opções de software/firmware adicionais. Contudo, é preciso muito cuidado para não sobrecarregar o roteador com a operação de serviços adicionais, como por exemplo, um firewall. Funcionalidades avançadas de firewalls, como VPN, DMZ, filtragem de conteúdo ou proteção antivírus, podem não estar disponíveis ou sua implementação pode ser muito dispendiosa.

Firewalls baseados em software

Normalmente, os firewalls baseados em software são aplicativos sofisticados e complexos, que são executados em servidores UNIX ou Windows NT dedicados. Esses produtos tornam-se dispendiosos quando se leva em consideração os custos associados ao software, sistema operacional dos servidores, hardware dos servidores e manutenção contínua exigida para suportar a implementação desses produtos.

É fundamental que os administradores monitorem constantemente a rede e instalem a versão mais recente do sistema operacional e de correções de segurança, assim que estiverem disponíveis. Sem essas correções para cobrir falhas recém-descobertas na segurança, o firewall de software pode acabar se tornando inútil.

Dispositivos de segurança dedicados

Muitos dispositivos de firewall são sistemas dedicados, baseados em hardware. Como esses dispositivos funcionam em um sistema operacional embutido, projetado especificamente para uso com firewalls, são menos suscetíveis às falhas de segurança, inerentes aos sistemas operacionais Windows NT e UNIX. Esses firewalls de alta performance são projetados para atender às altíssimas exigências de throughput ou ao uso intensivo de poder de processamento exigido pelos firewalls SPI.

Como não há necessidade de tornar o sistema operacional mais robusto, os dispositivos de firewall geralmente são mais fáceis de instalar e configurar do que os produtos de firewall de software, oferecem instalação “Plug-and-Play” e requerem pouca manutenção, sendo uma solução bastante completa. São também de excelente custo-benefício quando comparados a outras implementações de firewall.

Como projetar um firewall para sua rede

Quando você estiver familiarizado com os diferentes firewalls disponíveis no mercado, o passo seguinte será definir a política de firewall a ser adotada. Por exemplo, o firewall rejeitará explicitamente todos os serviços, exceto aqueles cruciais para a conexão à Internet? Ou o firewall se destina a fornecer um método de acesso comprovado com base em “formação de fila”, de modo que não envolva riscos? Decisões desse tipo dizem mais respeito à política do que à engenharia.

A decisão seguinte refere-se aos níveis de monitoração, redundância e controle desejados. Isso envolve cuidadosa análise das necessidades, inclusive avaliação de riscos, e a escolha entre requisitos muitas vezes conflitantes, a fim de decidir o que deve ser implementado.

No que diz respeito a firewalls, você deve dar ênfase à segurança, não à conectividade. Deve considerar o bloqueio geral como padrão e só

autorizar os serviços necessários após análise caso a caso. Se o você bloquear tudo exceto um conjunto específico de serviços, a tarefa se tornará bem mais fácil.

Conclusão

As falhas na segurança são bastante reais e extremamente perigosas. Hoje, todas as empresas estão cientes de que é fácil ser vítima de ataques deliberados ou aleatórios e do prejuízo que esses ataques podem causar. A boa notícia é que a 3Com Corporation está absolutamente ciente desses riscos e, por isso, está desenvolvendo soluções melhores e mais seguras. Empresas de pequeno e médio porte e escritórios remotos podem beneficiar-se das novas soluções de firewall propostas pela 3Com, que são mais fáceis e econômicas de administrar do que os firewalls convencionais.

Embora os firewalls sejam apenas um dos componentes do sistema de segurança como um todo, eles são fundamentais, e as empresas precisam dedicar o tempo que for necessário para decidir qual deles melhor atende a suas necessidades e instalá-lo o mais rápido possível. Os pontos vulneráveis na segurança são um risco constante, e não existe ocasião melhor do que o momento presente para proteger os valiosos dados de sua empresa.



3Com Corporation. Matriz: Av. Alfredo Egídio de Souza Aranha, 177 – São Paulo, SP – CEP 04726-170.

Para obter mais informações sobre as soluções da 3Com, visite o site www.3com.com. A 3Com Corporation é uma empresa de capital aberto cujas ações são negociadas na Nasdaq sob o símbolo COMS.

As informações contidas neste documento representam a visão atual da 3Com Corporation sobre os tópicos discutidos, na data desta publicação. Como a 3Com tem de responder às condições dinâmicas do mercado, esta publicação não deve ser interpretada como um compromisso por parte da 3Com e a 3Com não pode garantir a exatidão de quaisquer informações apresentadas após a data dessa publicação. Esse documento tem fins informativos; a 3Com não se responsabiliza pelas informações expressas ou implícitas neste documento.

Copyright © 2000 3Com Corporation. Todos os direitos reservados. O logotipo e o símbolo da 3Com são marcas registradas da 3Com. Windows NT é uma marca registrada da Microsoft. UNIX é uma marca comercial dos Laboratórios UNIX. Todos os outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.