



Firewalls

A Primeira Linha de Defesa



Hackers

- Se você tem um computador conectado à Internet, esteja certo de que ele se tornará alvo para algum Hacker.



Hackers

- Embora seja improvável que os Hackers visem especificamente seu computador, isso não significa que eles o deixarão em paz se por acaso o encontrarem quando estiverem procurando suas vítimas na Internet.



Hackers

- Gostam de alvos fáceis.
- Podem não estar interessados nas suas informações.
- Podem invadir seu computador apenas por diversão.
- Para treinar um ataque a uma máquina relativamente segura.
- Para usar seu disco rígido como armazenamento de arquivos ilegalmente copiados.
- Para implantar um programa “zumbi” no seu disco que possa comandar sua máquina para inundar determinado site com dados inúteis, que é conhecido como ataque de negação de serviço.



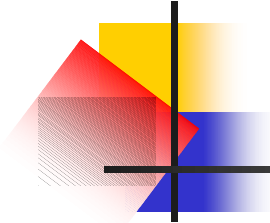
Hackers

- Seus dados podem ser inúteis, mas seu computador em si pode ainda ser um recurso valioso.



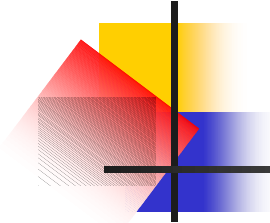
Firewalls

- Se você não gosta da idéia de alguém tomar controle do seu computador e ter a capacidade de apagar seus dados a qualquer momento, você precisa protegê-lo com um Firewall.



Conceito de Firewall destinados à rede

- Mecanismo de segurança interposto entre a rede interna (corporativa) e a rede externa (Internet), com a finalidade de liberar ou bloquear o acesso de computadores remotos - de usuários na Internet - aos serviços que são oferecidos dentro de uma rede corporativa.



Conceito de Firewall destinados à uma Máquina

- Também, temos os Firewalls Home, destinados a uma máquina ou uma estação de trabalho (workstation).



Firewalls

- Sendo um firewall o ponto de conexão com a Internet, tudo o que chega à rede interna deve passar pelo firewall.
- É responsável pela aplicação de regras de segurança, e em alguns casos pela autenticação de usuários, por “logar” tráfego para auditoria.
- É mecanismo obrigatório num projeto de segurança.



Firewalls

- No mínimo todo computador deveria ter um firewall, o qual age como uma porta trancada para manter intrusos vindos da Internet afastados do seu computador.



Firewalls

- Não propicia 100% de proteção contra hackers, mas pode protegê-lo contra boa parte dos hackers que espreitam endereços IP, procurando um computador vulnerável.



Firewalls

- Assim que um hacker encontra um computador sem um firewall, é relativamente fácil invadí-lo.
- Suscetíveis a ataques:
 - modem ADSL,
 - acesso discado



Firewalls

- Funcionam bloqueando as comunicações de/para seu computador.
- Muitos hackers usam scanners de portas para localizar alvos potenciais.
- Um firewall pode bloqueá-los para impedir que um hacker alcance seu computador.



Firewalls

- No nível mais simples um firewall bloqueia um scanner de portas, o que informa ao hacker que o firewall existe.



Firewalls

- Num nível mais complexo, um firewall pode mascarar a existência do seu computador, tornando-o invisível para hackers que usem scanners de portas.



Firewalls

- Neste caso, o hacker não saberá se encontrou um uma máquina protegido por firewall ou um endereço IP inválido.



Firewalls

- Em ambos os casos, é provável que o hacker deixe seu computador e procure um alvo mais fácil para atacar.



Firewalls

- Permitir que o tráfego legítimo passe através de um firewall.
- Critérios para bloquear tráfego ilegal:
 - endereços IP
 - protocolos
 - portas
 - programas específicos



Endereços IP

- Um firewall pode bloquear tráfego de certos endereços IP ou, ao contrário, somente aceitar conexões de endereços IP específicos (um computador corporativo confiável)



Protocolos

- Um firewall pode permitir somente a passagem do HTTP e bloquear o FTP, UDP, ICMP, SMTP e Telnet.



Protocolos

- UDP (User Datagram Protocol)

para transmitir informações que não requeiram uma resposta, como streaming de áudio ou vídeo.



Protocolos

- ICMP (Internet Control Message Protocol)

Relatar erros a outros computadores.



Protocolos

- SMTP (Simple Mail Transfer Protocol)

Para enviar e receber email.

- Telnet

Acessar e controlar um computador remoto.



Portas

- Permitem tipos de comunicações para dentro de um computador.
- Firewalls normalmente bloqueiam todas as portas, excetos a porta 80 (HTTP) e a porta 25 para enviar e receber emails.



Portas

- Fechando certas portas, um firewall pode impedir que um hacker invada o sistema através de uma porta que foi esquecida aberta, ou abra um porta obscura para transmitir informações do seu computador para o hacker.



Portas

- Fechando portas, apenas força-se os hackers direcionarem seus ataques para as portas abertas.
- Isso limita os tipos de ataques que hacker pode fazer.



Programas Específicos

- Servem para controlar o que um computador pode fazer através da Internet.
- Examinam programas que se conectam à Internet e permitem que se escolha quais terão sua permissão para se conectar. Se um firewall detecta um programa não permitido, ele o bloqueia e notifica o fato.



Programas específicos

- Bloqueando programas não autorizados, conseguem impedir que Cavalos de Tróia de acesso remoto (RAT's) se conectem secretamente um hacker e dêem a ele controle sobre seu computador.
- Pode permitir somente o navegador ou um programa de email.



Firewalls

- Podem detectar e bloquear programas **spyware** (programas de monitoração de desktop).
- **Spywares** podem capturar imagens de tela que mostram suas atividades, toques de teclas que são digitadas, rastrear programas utilizados, registrar quanto tempo se gasta usando cada programa, e transmitir esses registros, para um hacker ou alguém que esteja lhe espionando.



Bloqueando Tráfego Ilegal

- Combinando a filtragem de endereços IP, protocolos, portas ou mesmo de palavras ou frases específicas, firewalls podem bloquear a maioria das tentativas indesejadas de invadir um computador.

Firewalls em Hardware



- Netgear
<http://www.netgear.com>
- TRENDware
<http://trendware.com>
- D-Link
<http://www.dlink.com>



Firewalls em software para Windows

- Zone Alarm
<http://www.zonelabs.com>
- Tiny Personal Firewall
<http://www.tinysoftware.com>
- Sygate Personal Firewall
<http://soho.sygate.com>
- Personal Firewall
<http://www.mcafee.com>



Firewalls em software para Windows

- Look 'n' Stop
<http://www.looknstop.com>
- Norton Internet Security
<http://www.symantec.com>
- Outpost Firewall
<http://www.agnitum.com>



Firewalls em Software

- Muitas versões do LINUX vêm com um firewall.
- O Windows XP também tem um firewall.



Firewalls em Software

- Desenvolver um Firewall para LINUX:
Falcon Firewall Project
<http://falcon.naw.de>
- Estudando o código-fonte deste firewall, pode-se obter o entendimento de como firewalls funcionam e modificá-lo para proteger-se de ameaças mais recentes na Internet.



Problemas com Firewalls

- Os novatos não têm idéia de como avaliá-los.
- Como leva tempo para configurá-los, a maioria dos usuários iniciantes provavelmente irão configurá-lo de forma errada, dando um falso senso de segurança.



Problemas com Firewalls

- Só se consegue proteger conexões chegando e saindo do computador via Internet.
- Nada pode ser feito para impedir o acesso por uma linha telefônica, através de um dispositivo de acesso sem fio, ou através do teclado se alguém estiver fisicamente usando o computador.



Problemas com Firewalls

- Firewalls podem ser enganados.

Por exemplo, um hacker poderia renomear um Cavalo de Tróia de acesso remoto, que acesse a Internet, de forma que ele tenha o mesmo nome que um programa na lista dos programas permitidos, como por exemplo, um navegador Web.



Problemas com Firewalls

- Podem ser contornados com uma técnica chamada “túnel de firewall”, que simplesmente usa quaisquer portas e protocolos permitidos pelo firewall.



Problemas com Firewalls

- Dois produtos que permitem “túnel de firewall”:

RemFTP

<http://www.remftp.com>

HTTP-Tunnel

<http://www.http-tunnel.com>



Problemas com Firewalls

- Configurar seu firewall corretamente, e assim, deixar buracos nas defesas do seu computador, simplesmente porque o firewall pode não ter certas funções imprescindíveis, que outro talvez ofereça.



Avaliando Firewalls

- Aprender sobre detalhes, escolher o melhor para você, comparações técnicas:

Home PC Firewall Guide

<http://www.firewallguide.com>

Firewall.com

<http://firewall.com>



Avaliando Firewalls

Firewall.net

<http://www.firewall-net.com>

Free-Firewall.org

<http://www.free-firewall.org>



Firewalls

- Enquanto, não experimentar vários firewalls diferentes, você nunca poderá saber quão indefeso, determinado firewall acabará sendo.



Testar a capacidade de Firewalls

- LeakTest

<http://grc.com/lt/leaktest.htm>

- FireHole

<http://keir.net/firehole.html>

- OutBound

<http://www.hackbusters.net/ob.html>

- PC Flank

<http://www.pcflank.com>



Testar a capacidade de Firewalls

- Port Detective
<http://www.portdetective.com>
- YALTA
http://www.soft4ever.com/security_test/En/index.htm
- TooLeaky
<http://tooleaky.zensoft.com>
- Um programa de teste pode dizer se o firewall está protegendo o seu computador.



Fortalecendo o Sistema Operacional

- Além de instalar um firewall, certifique-se de atualizar o sistema operacional com os patches de segurança mais atuais.
- Os hackers descobrem rapidamente todas as falhas em determinado sistema operacional, e se as encontram podem ser capazes de explorá-las, independentemente de qualquer firewall instalado.