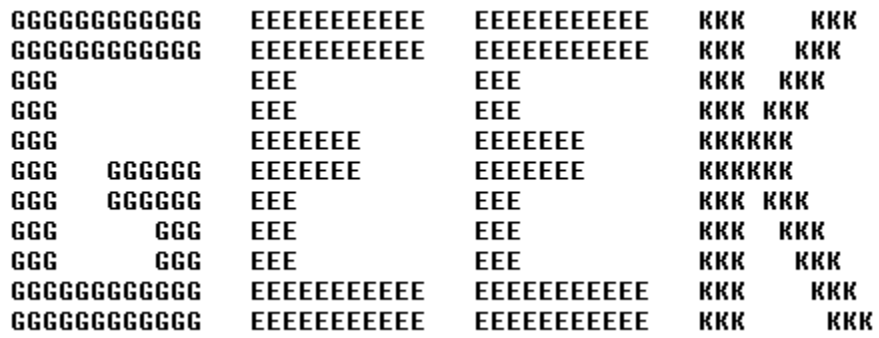

GeekBrasil
http://www.geekbrasil.com.br

```
#################################################################
#                                                               #
# writed by steel_edge (steel_edge@geekbrasil.com.br)           #
# icq - 86818424                                                #
#                                                               #
# copyright http://www.geekbrasil.com.br                        #
#                                                               #
# se voce for copiar este texto, ou parte dele, favor           #
# colocar o nome do autor deste texto e tambem de onde          #
# ele foi retirado                                              #
#                                                               #
#################################################################
```

```
*********************************************
*                                           *
*  todo o conteudo deste texto eh somente   *
*  para fins de aprendizado, nao nos        *
*  responsabilizamos pelo mau uso das       *
*  informacoes aqui contidas nem por atos   *
*  que voce venha a cometer.                *
*                                           *
*********************************************
```

Firewalls

/* writed by steel_edge */
/* steel_edge@inferno.com */

neste txt pretendo demonstrar por altos o funcionamento basico de um firewall, sem se aprofundar muito no assunto, se voce procura maiores informações recomendo a leitura das documentacoes diretamente nos sites das empresas que produzem este tipo de software.
topicz
======

-intro

-filtragem de pacotes

-mascaramento de ip

-autenticacao criptografada

-tunel criptografado

intro
=====

firewalls sao programas utilizados para manter uma conexao de uma rede local com as redes externas a mais segura possivel. os firewalls se localizam nas interconexoes (gateways) de redes e por esse motivo os firewalls sao considerados uma protecao importante.
firewalls criam passagens entre as redes interna e externa para que todo o trafego entre uma rede e outra tenha que passar por um unico ponto de controle, e como as conexoes de linhas diretas externas sao relativamente lentas se comparadas com a velocidade atual do computadores, a latencia causada pelos firewalls pode ser considerada transparente.

basicamente sao cinco as maneiras de operacao dos firewalls:
filtragem de pacotes - rejeita pacotes tcp/ip de hosts nao autorizados e rejeita tentativas de conexao com servicos nao autorizados.

nat (network address translation) - mascaramento de rede, ou seja, o firewall realiza a conversao dos enderecos ip's dos hosts internos para oculta-los de qualquer monitoracao externa.

servidor proxy - faz com que as conexoes de aplicativos del alto nivel em beneficio de hosts internos quebrem completamente a conexao da camada de rede entre o host interno e externo.

autenticacao criptografada - permite aos usuarios da rede publica provarem sua identidade ao firewall a fim de obter acesso a rede privada a partir de pontos externos.

tuneis criptografados - estabelecem uma conexao segura entre duas redes privadas por meio de um meio publico como a internet, isso permite que redes fisicamente separadas utilizem a internet ao inves de linhas diretas para comunicarem-se entre si.

filtros de pacotes
==========

os filtros de pacotes comparam os pacotes dos protocolos de rede (como o ip) e os protocolos de transporte (como o tcp) com um conjunto de regras contidas em um banco de dados e soh encaminham os pacotes que atendam aos criterios. estes filtros podem ser implementados em roteadores ou em pilhas tcp/ip dos servidore.
os filtros implementados dentro de roteadores evitam que o trafego suspeito alcance a rede de destino protegendo todas as maquinas da rede, enquanto os modulos de filtro tcp/ip nos servidores evitam que maquinas especificas respondam ao trafego suspeito, o trafego ainda assim alcanca a rede e poderia atingir qualquer maquina dela.

filtragem de sistema operacional
==========

a maioria dos sistemas unix e windows nt server incluem a filtragem de pacotes na interface do protocolo tcp/ip, essa filtragem pode ser usada em conjunto com um firewall para controlar o acesso aos servidores individuais, essa filtragem tambem pode ser usada para oferecer uma medida adicional de segurança interna. como apenas a filtragem nao eh o suficiente para proteger toda a rede, a filtragem interna do sistema operacional nao eh suficiente para criar um ambiente totalmente seguro.
a filtragem basica do sistema operacional permite definir criterios de aceitacao de cada adaptador de rede presente no computador nas conexoes de entrada com base em:

- numero do ip
- numero da porta tcp
- numero da porta udp

geralmente a filtragem nao se aplica as conexoes para fora e eh definida separadamente para cada adaptador do sistema.

mascaramento de ip
==========

o mascaramento de ip's serve para ocultar host's interno, o mascaramento de ip na verdade eh um proxy, um unico host faz as solicitacoes em nome de todos os host's internos, ocultando assim suas identidades na rede publica (internet). o windows nt nao fornece essa funcao, sendo que voce precisa utilizar um firewall para realizar esta tarefa.

p.s. o windows nt nao aceita mascaramento de ip, mas o 2000 sim.

o mascaramento de ip converte todos os os enderecos de host's internos para o endereco do firewall, entao o firewall retransmite os dados dos host's internos a partir de seu proprio endereco usando o numero da porta tcp para saber quais conexoes do lado publico devem ir para os host's internos. o mascaramento de ip consegue ocultar eficientemente todas as informacoes sobre o tcp/ip dos host's internos de pessoas que desejem obter estas informacoes, o mascaramento tambem permite usar qualquer intervalo de enderecos ip desejados na rede interna, mesmo que esses enderecos jah estejam sendo utilizados em qualquer outro lugar da internet. o mascaramento pode ainda multiplicar um unico endereco ip por toda uma rede.

proxies
=======

o mascaramento de ip resolver muitos problemas relacionados com conexoes
diretas via internet, mas ainda assim nao restringe completamente o fluxo de datagramas por meio do firewall. eh possivel que alguem com um monitor de rede (sniffer) observe o trafego saindo do firewall e determine que estah convertendo enderecos para outras maquinas, assim eh possivel que alguem comande as conexoes tcp ou engane as conexoes de retorno por meio do firewall.
os proxies em nivel de aplicativos impedem que isso aconteca, eles permitem desconectar o fluxo de protocolos em nivel de rede por meio do firewall e restringir o trafego somente para protocolos como o http e ftp.

os proxies substituem as tentativas de conexao a servidores dirigidas para fora e depois fazem a solicitacao para o servidor de destino real em nome do cliente. quando o servidor retorna os dados o proxy transmite esses dados para o cliente, os proxies realizam essecialmente um tipo de ataque como se houvesse alguem no meio do caminho, e sao um bom exemplo de como qualquer roteador entre voce e o outro sistema de ponta poderia realizar qualquer tipo de processamento sem autorizacao.

tuneis criptografados
==========

os tunei criptografados permitem conectar com seguranca duas redes separadas fisicamente pela internet sem expor os dados a sniffers, os tuneis criptografados poderiam estar sujeitos a tentativas de redirecionamento, inicio de conexoes falsas e outros tipos de hacking enquanto o tunel estivesse sendo estabelecido, porem quando implementados como parte integrande de um firewall os servicos de autenticacao e seguranca do firewall poder ser usados para evitar a exploracao do tunel quando ele estiver sendo estabelecido, e uma vez estabelecidos os tuneis sao impenetraveis, enquando a criptografia for segura :O)

autenticacao criptografada
==========

a autentificacao criptografada permite que usuarios externos provem ao firewall que eles sao usuario autorizados a abrir uma conexao por meio do firewall com a rede interna.
o uso de autentificacao criptografada eh conveniente porque ela ocorre no nível de transporte entre um pacote de software cliente e o firewall, quando for estabelecida a conexao, todo software aplicativo e todo software de logon no sistema operacional serao executados.

\!!!!!!/
(õ õ)
----------oOOO--(_)----------
| Arquivo baixado da GEEK BRASIL |
| O seu portal de informática e internet |
| http://www.geekbrasil.com.br |
| Dúvidas ou Sugestões? |
| webmaster@geekbrasil.com.br |
----------oOOO----------
|__| |__|
|| ||
ooO Ooo