FIREWALLS

A Primeira Linha de Defesa

Como montar uma estrutura de firewall que impeça invasões.

POR QUE FIREWALL ?

Hoje, o mundo respira Internet.

A Internet que o mundo respira não é segura.

Security Module (2003):

- Pesquisa Nacional de Segurança da Informação.
- 60% : Internet é o principal ponto de invasão.
- 78% : ameaças, riscos e ataques tendem a aumentar em 2004.
- 32% : crackers são os principais invasores.
- 26% : não conseguem identificar os responsáveis.
- Número de empresas com ataques e invasões:
  43% (2002) e 77% (2003).

POR QUE FIREWALL ?

Internet

Uma imensa **rede descentralizada** e **não gerenciada**, rodando sob uma **suíte de protocolos denominada IPv4**, que **não foi projetada para assegurar a integridade** das informações e **realizar controles de acesso.**

POR QUE FIREWALL ?

De que forma um software denominado **Firewall** consegue mudar este paradigma ?

Existem **diversas formas de se violar uma rede,** mas essas formas nada mais fazem do que se aproveitar de **falhas em serviços de rede e protocolos.**

POR QUE FIREWALL ?

Mas o que um Firewall poderá fazer por tais serviços e protocolos ?

Neste sentido, pouco será a utilidade de um Firewall.

Um Firewall não pode corrigir erros em serviços e protocolos.

Mas, se **disponibilizarmos todos os serviços que precisamos e limitarmos seu uso** apenas a redes autorizadas ou a certos hosts confiáveis ?

POR QUE FIREWALL ?

Quem fará essa separação ?

Quem bloqueará conexões desconhecidas e não autorizadas em minha rede ?

Esta é uma das utilidades de um Firewall.

Sem um Firewall, cada host na rede interna, seria responsável por sua própria segurança.

Sendo o único computador diretamente conectado à Internet, poderá de forma segura levar serviços de inter-conectividade à rede interna.

POR QUE FIREWALL ?

Um Firewall não possui a função de vasculhar pacotes a procura de assinaturas de vírus.

Um Firewall poderá evitar que a rede interna seja monitorada por Trojans e que os mesmos troquem informações com outros hosts na Internet.

Poderá evitar que a rede interna seja vasculhada por um scanner de portas.

POR QUE FIREWALL ?

Poderá bloquear qualquer tentativa de conexão vinda da Internet para um host na rede interna.

Mas, as ameaças estão tão somente na Internet ?

FBI : 90% das invasões bem sucedidas a servidores corporativos, os usuários da rede (autorizados) tiveram algum nível de parcela de culpa.

- senhas mal escolhidas.
- usuários descontentes.

POR QUE FIREWALL ?

As ameaças passam a vir de todos os lados: **Internet** e **rede interna** (corporativa).

Um firewall poderá bloquear tanto o acesso externo, como acesso interno, liberando apenas para algumas máquinas.

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 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).

Exemplo: ZoneAlarm para Windows.

FIREWALLS

Sendo um firewall o ponto de conexão com a Internet, tudo o que chega à rede interna deve passar pelo firewall.

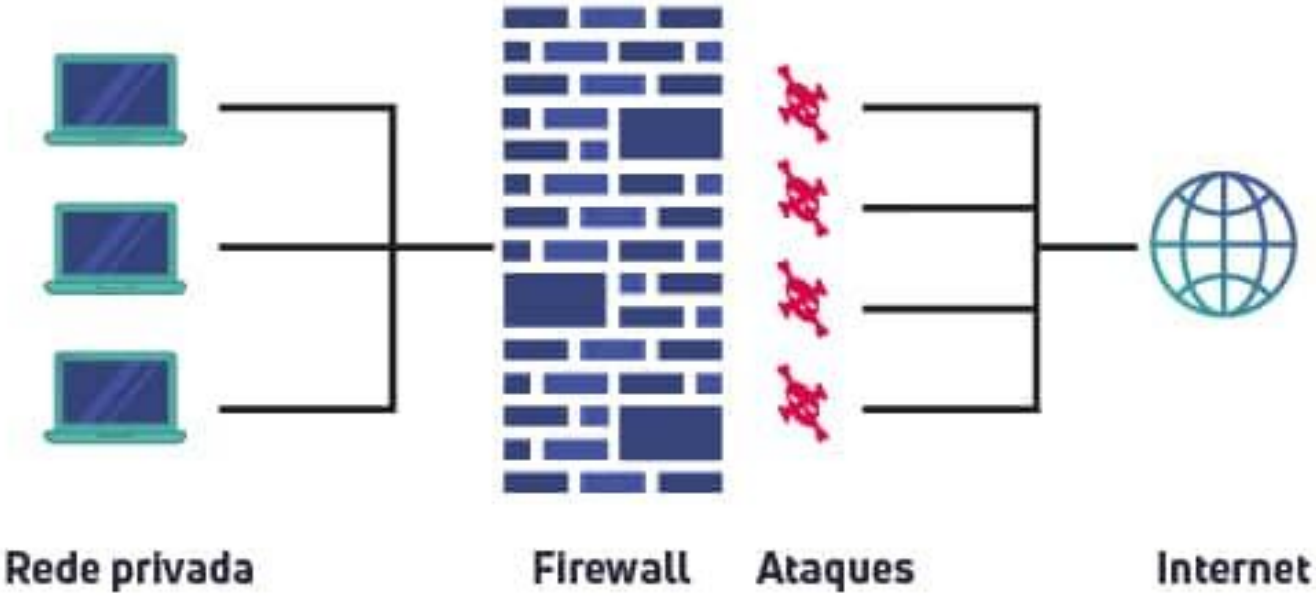
É responsável pela aplicação de regras de segurança.

E em alguns casos pela autenticação de usuários, por "logar" tráfego para auditoria.

É mecanismo obrigatório num projeto de segurança.

POR QUE FIREWALL ?

Um Firewall poderá especificar **que tipos de protocolos e serviços de rede serão disponibilizados,** tanto externa quanto internamente.



POR QUE FIREWALL ?

Um Firewall pode **controlar os pacotes de serviços não confiáveis:**

- rlogin,
- telnet,
- FTP,
- NFS,
- DNS,
- LDAP,
- SMTP,
- RCP,
- X-Window.

POR QUE FIREWALL ?

Pode realizar compartilhamento de acesso à Internet a toda a rede interna sem permitir a comunicação direta entre as mesmas.

Bloquear acesso indevido a sites e hosts não-autorizados.

POR QUE FIREWALL ?

Porque as empresas devem se conectar à Internet com algum nível de preparo específico para este fim.

LEMBRANDO ...

Nada evitará que ameaças, ataques e invasões continuem a existir.

O que definirá se serão bem sucedidas ou não será o conhecimento embutido em seu Firewall e demais ferramentas de segurança.

KERNEL E FIREWALL

Tudo o que chega ou sai de um computador é processado pelo kernel do sistema operacional desse computador.

No **Linux,** as **funções de Firewall são agregadas à própria arquitetura do kernel.**

O Linux tem a capacidade de transformar o Firewall no próprio sistema.

FIREWALL NO LINUX

No Linux, não é preciso comprar um Firewall corporativo caríssimo.

Firewall é *open source*, gratuito.

DÚVIDAS?