Arquitetura e Organização de Sistemas Computadorizados - Firewall

Osmar de Oliveira Braz Junior

Márcia Cargnin Martins Giraldi

Objetivos

- Apresentar o que é Firewall e sua importância para a segurança da informação.
  - Tipos e arquiteturas

Firewall

Firewall

- **Internet** não é um “território” livre de perigos
- É importante conhecer e utilizar **ferramentas** de proteção para computadores e redes
- Vamos adentrar em uma das opções de segurança mais importantes dos ambientes computacionais: o **Firewall**

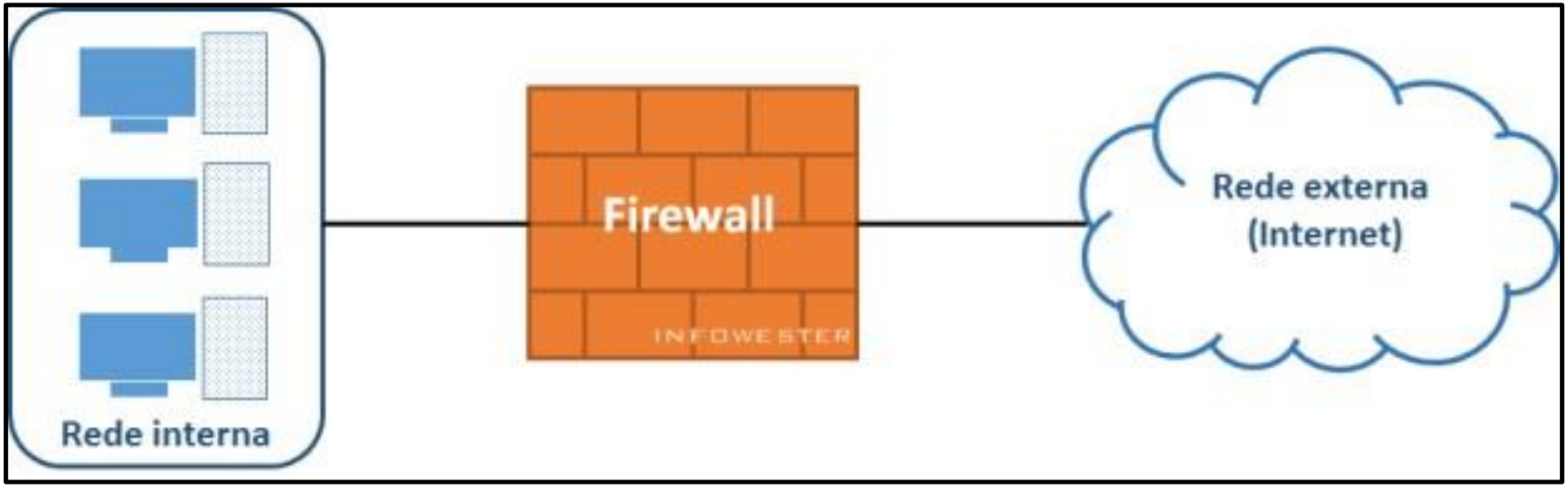
Firewall – Definição

- De acordo com Zwicky, Cooper e Chapman (2000), **firewalls** podem ser definidos como barreiras interpostas entre a rede privada e a externa com a finalidade de evitar intrusos (**ataques**); isto é, são mecanismos (**dispositivos**) de segurança que protegem os recursos de hardware e software, da empresa, dos perigos (**ameaças**) aos quais o sistema está exposto.

Firewall – Definição

- Solução de segurança baseada em hardware ou **software** (mais comum)
- A partir de um conjunto de **regras** ou **instruções**(política da empresa), analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas
- "**Parede de fogo**", a tradução **literal** do nome, já deixa claro se enquadra em uma espécie de barreira de defesa
- O objetivo consiste basicamente em **bloquear tráfego** de dados **indesejado** e liberar acessos bem-vindos

Firewall



Firewall – O que e como?

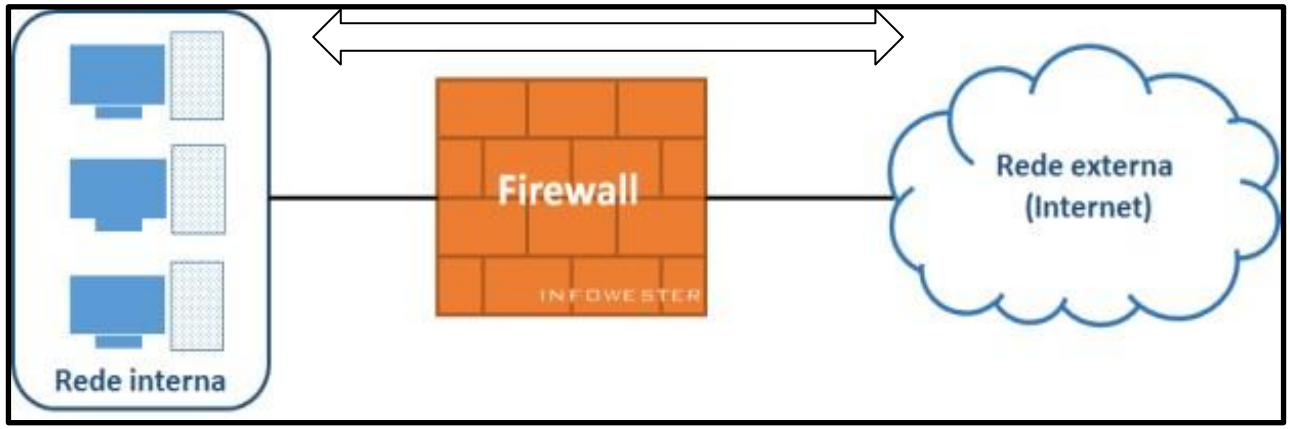
- Quando se está construindo um **firewall**, a primeira coisa com que você deve se preocupar é o que e como proteger.
  - **dados** – são as informações armazenadas nos computadores da empresa, às quais devem-se garantir confidencialidade, integridade e disponibilidade;
  - **recursos** – são os próprios computadores, evitando danos lógicos aos equipamentos e a utilização dos recursos da empresa, como por exemplo, roubo de CPU;
  - **a reputação da empresa** – a reputação é fundamental para o negócio da empresa. Imagine o site da presidência com informações inverídicas, ou imagine a situação de alguém fazer uso do e-mail de uma pessoa para enviar informações, ou denegrir a imagem de pessoas ou instituições.

Firewall – O que e como?

- Um **firewall** previne que danos provenientes da internet se espalhem pela rede interna.
- Ele serve para vários **propósitos**:
  - **restringe** o **acesso** de usuários externos à rede interna. A verificação é realizada cuidadosamente, via um ponto de controle;
  - **previne ataques**; e
  - **restringe** que **usuários** internos da rede tenham acesso à internet e sites não autorizados.

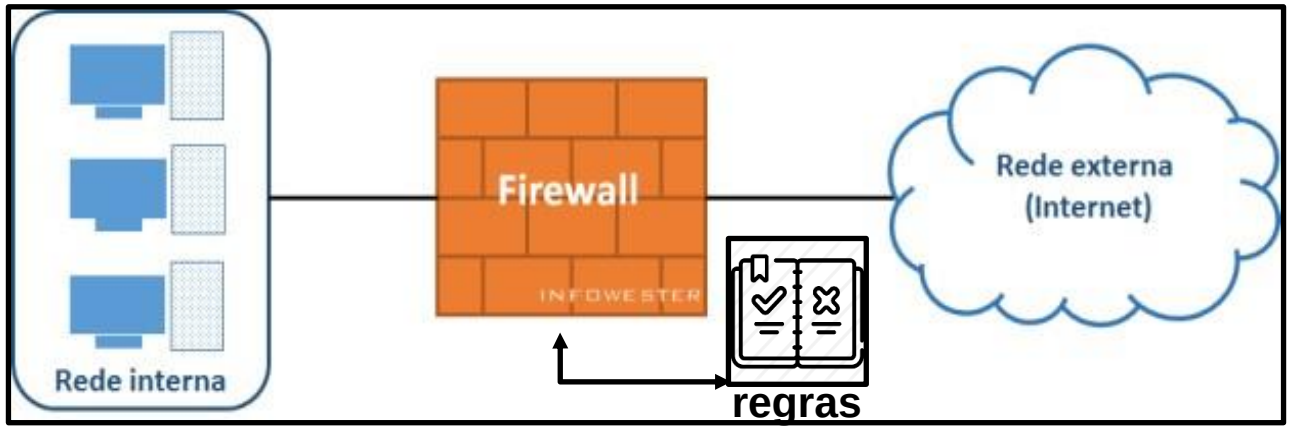
Firewall - Funcionamento

- **Firewall** atua como uma espécie de **barreira** que verifica quais dados podem passar ou não.
- Todo e qualquer tráfego que chega ou sai da rede interna, por exemplo, tem de passar pelo **firewall**.



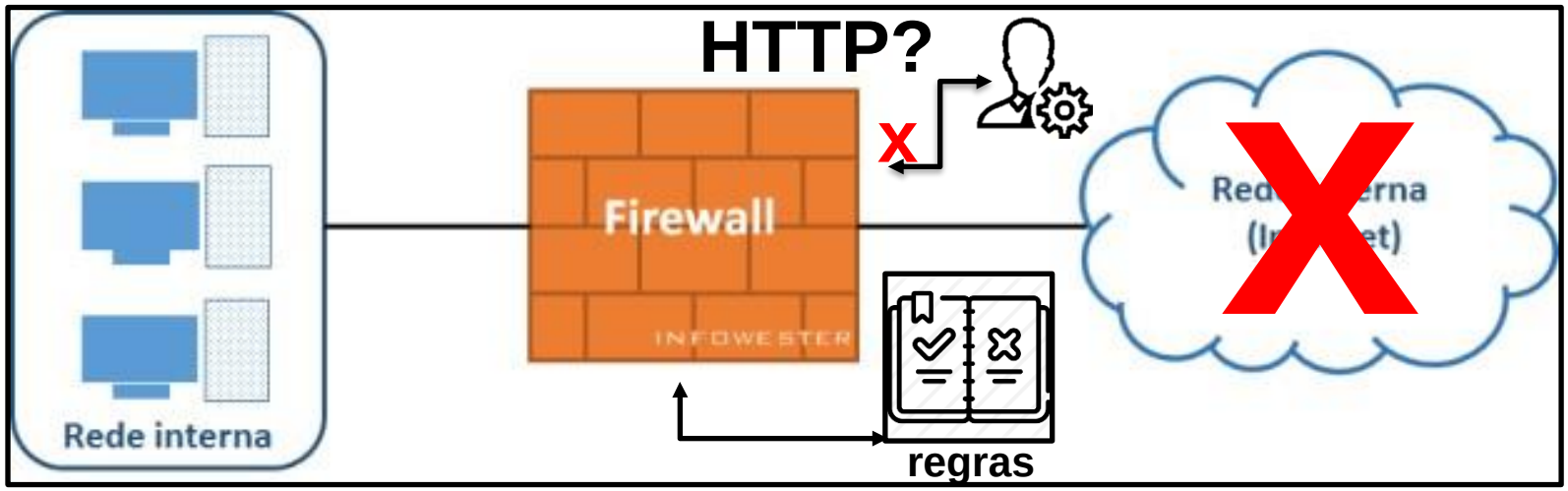
Firewall - Funcionamento

- No **firewall** estão implementadas todas as **regras** que permitem o tráfego de e-mails, transferência de arquivos, logins remotos etc.



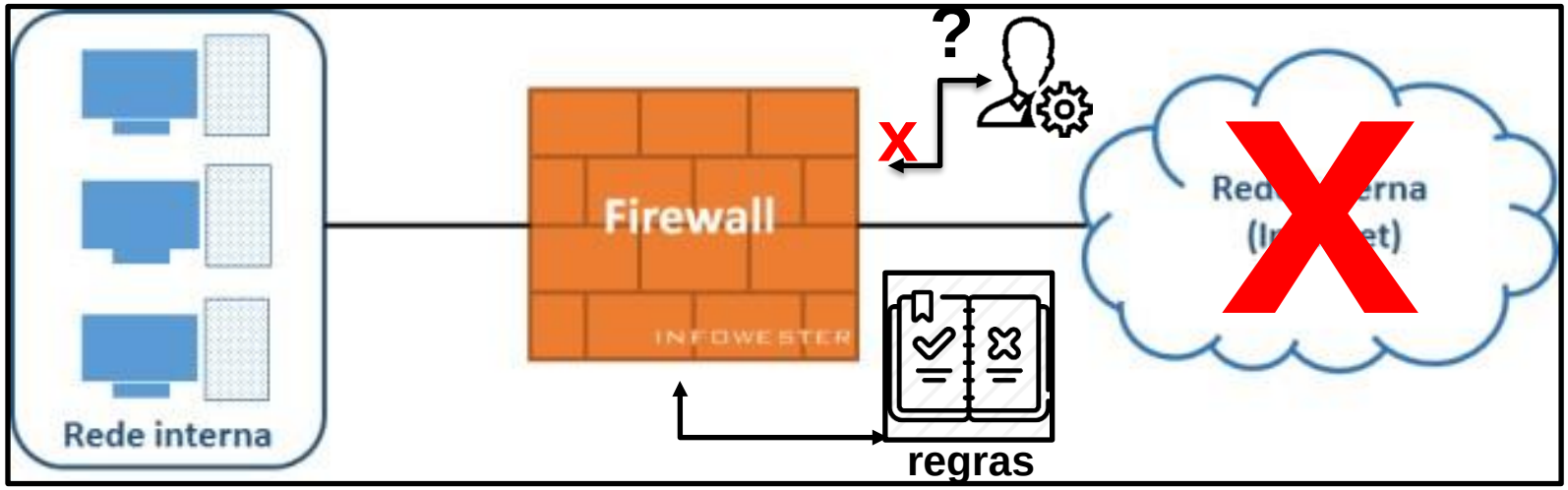
Firewall - Funcionamento

- Em um modo mais restritivo, um firewall pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede. O problema é que esta condição isola este computador ou esta rede, então pode-se criar uma regra para que, por exemplo, todo aplicativo aguarde autorização do usuário ou administrador para ter seu acesso liberado. Esta autorização poderá inclusive ser permanente: uma vez dada, os acessos seguintes serão automaticamente permitidos



Firewall - Funcionamento

- Em um modo mais versátil, um firewall pode ser configurado para permitir automaticamente o tráfego de determinados tipos de dados, como requisições HTTP (sigla para *Hypertext Transfer Protocol* – protocolo usado para acesso a páginas Web), e bloquear outras, como conexões a serviços de e-mail



Firewall - Funcionamento

- **Firewalls** mais avançados podem ir além, direcionando determinado tipo de tráfego para sistemas de segurança internos mais específicos ou oferecendo um **reforço extra** em procedimentos de autenticação de usuários, por exemplo

Firewall - Tipos

- O trabalho de um **firewall** pode ser realizado de várias formas.
- O que define uma **metodologia** ou outra são fatores como **critérios** do desenvolvedor, necessidades específicas do que será protegido, **características** do sistema operacional que o mantém, **estrutura da rede** e assim por diante
- Por causa dessa **diversidade** de metodologias podemos encontrar mais de um tipo de **firewall**.
- A seguir, os mais conhecidos.

Firewall - Filtragem de pacotes (*packet filtering*)

- As primeiras soluções de firewall surgiram na década de 1980 baseando-se em filtragem de pacotes de dados (*Packet filtering*)
- metodologia mais simples e, por isso, mais limitada, embora ofereça um nível de segurança significativo
- é importante saber que cada pacote possui um cabeçalho com diversas informações a seu respeito:
  - endereço IP de origem e destino,
  - tipo de serviço,
  - tamanho,
  - entre outros

- O Firewall então analisa estas informações de acordo com as regras estabelecidas para liberar ou não o pacote (seja para sair ou para entrar na máquina/rede), podendo também executar alguma tarefa relacionada, como registrar o acesso (ou tentativa de) em um arquivo de log

Firewall - Filtragem de pacotes (*packet filtering*)

- A transmissão dos dados é feita com base no padrão TCP/IP (*Transmission Control Protocol/Internet Protocol*), que é organizado em camadas
- A filtragem normalmente se limita às camadas de rede e de transporte:
- a primeira é onde ocorre o endereçamento dos equipamentos que fazem parte da rede e processos de roteamento, por exemplo;
- a segunda é onde estão os protocolos que permitem o tráfego de dados, como o TCP e o UDP (*User Datagram Protocol*).
- Um firewall de filtragem pode ter, por exemplo, uma regra que permita todo o tráfego da rede local que utilize a porta UDP 123, assim como ter uma política que bloqueia qualquer acesso da rede local por meio da porta TCP 25

Firewall - Filtragem de pacotes (*packet filtering*)

- É possível encontrar dois tipos de firewall de filtragem de pacotes
- O primeiro utiliza o que é conhecido como **filtros estáticos**, enquanto que o segundo é um pouco mais evoluído, utilizando **filtros dinâmicos**

Firewall - Filtragem de pacotes (*packet filtering*)

- **Filtragem Estática:**
- Os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro
- A princípio, esta abordagem não é um problema, mas determinados serviços ou aplicativos podem depender de respostas ou requisições específicas para iniciar e manter a transmissão
- É possível então que os filtros contenham regras que permitem o tráfego destes serviços, mas ao mesmo tempo bloqueiem as respostas/requisições necessárias, impedindo a execução da tarefa
- Esta situação é capaz de ocasionar um sério enfraquecimento da segurança, uma vez que um administrador poderia se ver obrigado a criar regras menos rígidas para evitar que os serviços sejam impedidos de trabalhar, aumentando os riscos de o firewall não filtrar pacotes que deveriam ser, de fato, bloqueados

Firewall - Filtragem de pacotes (*packet filtering*)

- **Filtragem Dinâmica:**
- A filtragem dinâmica surgiu para superar as limitações dos filtros estáticos
- Nesta categoria, os filtros consideram o contexto em que os pacotes estão inseridos para “criar” regras que se adaptam ao cenário, permitindo que determinados pacotes trafeguem, mas somente quando necessário e durante o período correspondente
- Desta forma, as chances de respostas de serviços serem barradas, por exemplo, cai consideravelmente.

Firewall - Filtragem de pacotes (*packet filtering*)

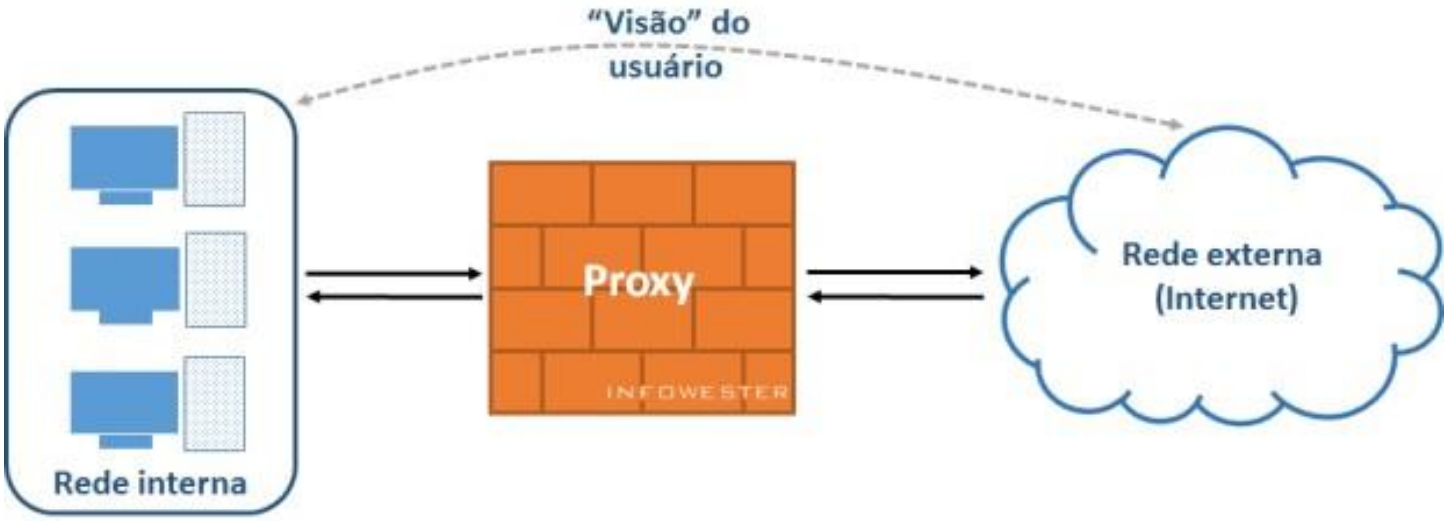
- O processo de **filtragem de pacotes** acarreta um **overhead** no sistema; e, numa situação de alto tráfego, torna-se necessário que se utilize um roteador com uma velocidade de processamento compatível.
- A filtragem de pacotes que a maioria dos *screening routers* realizam, é baseada no:
  - endereço IP de origem;
  - endereço IP de destino;
  - protocolo: se o pacote é TCP, UDP ou ICMP;
  - portas TCP ou UDP de origem;
  - portas TCP ou UDP de destino;
  - tipo da mensagem ICMP;
  - tamanho do pacote.

Firewall de aplicação ou proxy de serviços (*proxy services*)

- O firewall de aplicação, também conhecido como **proxy de serviços** (*proxy services*) ou apenas **proxy** é uma solução de segurança que atua como intermediário entre um computador ou uma rede interna e outra rede, externa – normalmente, a internet
- Geralmente instalados em servidores **potentes** por precisarem lidar com um grande número de solicitações, firewalls deste tipo são opções interessantes de segurança porque não permitem a comunicação direta entre origem e destino

Firewall de aplicação ou proxy de serviços (*proxy services*)

- Perceba que em vez de a **rede interna** se comunicar **diretamente** com a internet, há um **equipamento entre ambos** que cria duas conexões: **entre** a rede e o proxy; e **entre** o proxy e a internet

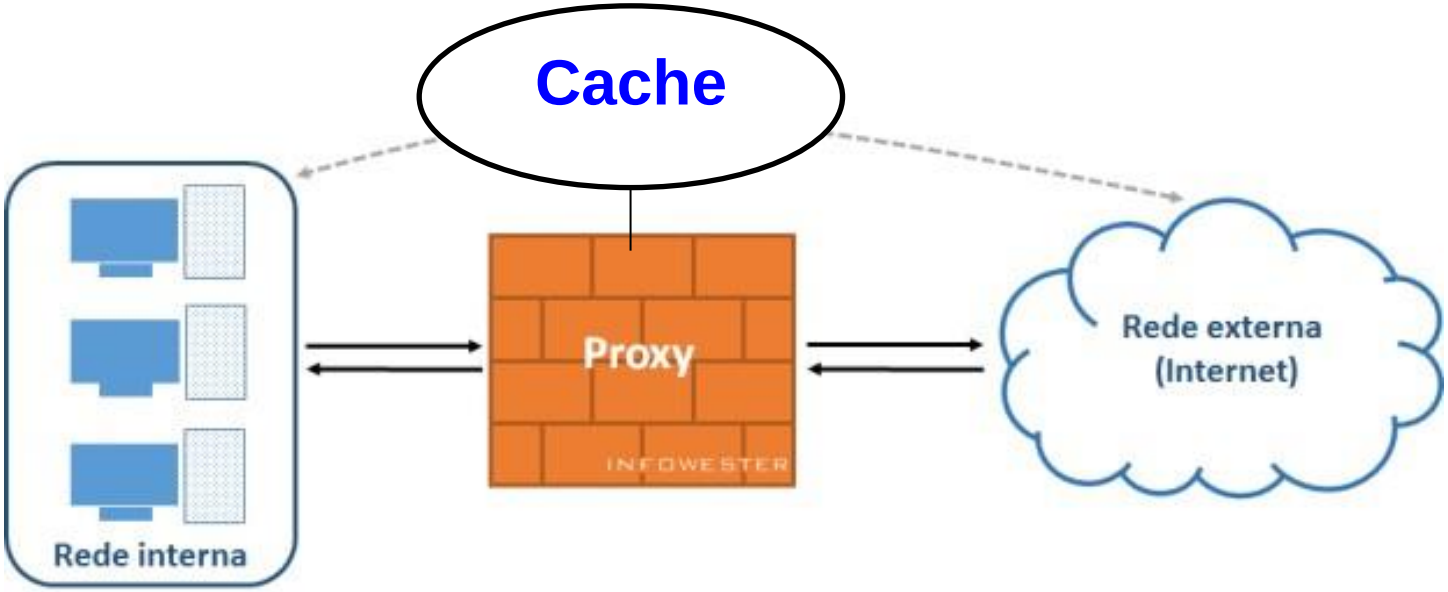


Cliente *proxy*

Servidor proxy

Firewall de aplicação ou proxy de serviços (*proxy services*)

- Os proxies, além de tornarem a rede mais segura, podem também deixá-la com maior **desempenho**.
- Essa eficiência vem com base na utilização dele como **cache** de informações solicitadas pelo usuário.



Firewall de aplicação ou proxy de serviços (*proxy services*)

- Perceba que todo o fluxo de dados **necessita** passar pelo proxy.
- Desta forma, é possível, por exemplo, estabelecer **regras** que impeçam o acesso de determinados endereços externos, assim como que proíbam a comunicação entre computadores internos e determinados serviços remotos.

Firewall de aplicação ou proxy de serviços (*proxy services*)

- Este controle amplo também possibilita o uso do **proxy** para tarefas complementares, como registro de tráfego de dados em arquivo de log, e auxiliar com conteúdo muito requisitado
- A **implementação** de um proxy não é tarefa fácil
- Este **tipo de firewall** não consiga ou exija muito trabalho de configuração para bloquear ou autorizar determinados acessos

Firewall de aplicação ou proxy de serviços (*proxy services*)

- O proxy "tradicional" exige que determinadas **configurações** sejam feitas nas ferramentas que utilizam a rede (por exemplo, um navegador de internet) para que a comunicação aconteça sem erros.
- O problema é, **dependendo** da aplicação, este trabalho de ajuste pode ser inviável ou custoso.

Firewall de aplicação ou proxy de serviços (*proxy services*)

- O proxy transparente surge como uma alternativa para estes casos porque as máquinas que fazem parte da rede não precisam saber de sua existência, dispensando qualquer configuração específica

- Todo acesso é feito normalmente **do cliente** para a rede externa e vice-versa, mas o proxy transparente consegue interceptá-lo e responder adequadamente, como se a comunicação, de fato, fosse direta

Firewall de aplicação ou proxy de serviços (*proxy services*)

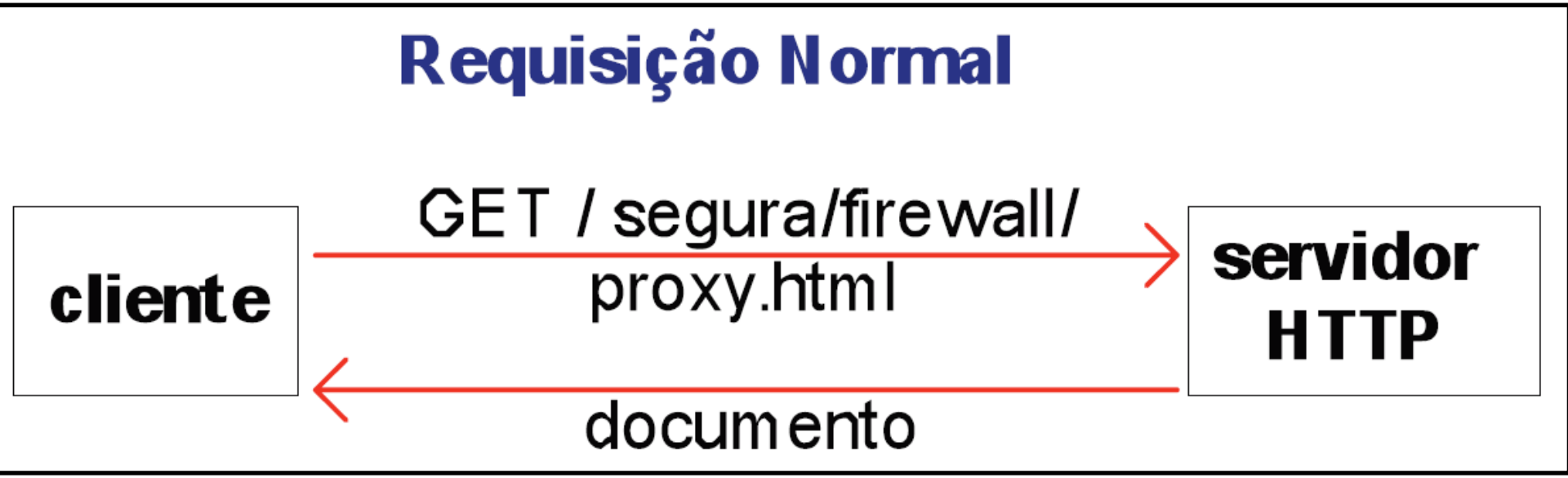
- **Desvantagem do Proxy Transparente:**
- Um proxy “normal” é capaz de barrar uma atividade maliciosa, como um malware enviando dados de uma máquina para a internet;
- O proxy transparente, por sua vez, pode não bloquear este tráfego
- Não é difícil entender: para conseguir se comunicar externamente, o malware teria que ser configurado para usar o proxy “normal” e isso geralmente não acontece; no proxy transparente não há esta limitação, portanto, o acesso aconteceria normalmente

Firewall de aplicação ou proxy de serviços (*proxy services*)

- Exemplo de requisição HTTP **sem** Proxy:
  - o cliente realiza a requisição http;
  - o servidor faz uso somente do *path* e a “porção-chave” da URL requisitada;
  - o tipo do protocolo “http:” e o nome do servidor são claros para o servidor HTTP remoto;
  - o *path* requisitado especifica um documento no sistema de arquivos local do servidor; ou, ainda, algum outro recurso disponível daquele servidor.

Firewall de aplicação ou proxy de serviços (*proxy services*)

- Requisição do usuário:
  - http://www.teste.com.br/segura/firewall/proxy.html
  - O *browser* converte para: GET / segura/firewall/proxy.html



Firewall de aplicação ou proxy de serviços (*proxy services*)

- Exemplo de uma requisição HTTP **com** proxy:
  - o cliente realiza a requisição HTTP com proxy;
  - o cliente especifica toda a URL para o proxy; com isso, o proxy possui todas as informações necessárias para realizar a requisição ao servidor remoto especificado na URL.

Firewall de aplicação ou proxy de serviços (*proxy services*)

- Requisição do usuário:
  - http://www.teste.com.br/segura/firewall/proxy.html
  - O **browser** converte para:
  - GET http://www.teste.com.br/segura/firewall/proxy.html
  - O *browser* se conecta ao servidor proxy.
  - O servidor proxy realiza a conexão com o servidor de internet, convertendo a requisição para:
  - GET / segura/firewall/proxy.html

Firewall de Inspeção de estados (*stateful inspection*)

- Tido por alguns especialistas no assunto como uma evolução dos filtros dinâmicos
- Este tipo de firewall trabalha fazendo uma espécie de comparação entre o que está acontecendo e o que é esperado para acontecer
- Para tanto, firewalls de inspeção analisam todo o tráfego de dados para encontrar estados, isto é, padrões aceitáveis por suas regras e que, a princípio, serão usados para manter a comunicação. Estas informações são então mantidas pelo firewall e usadas como parâmetro para o tráfego subsequente

Firewall de Inspeção de estados (*stateful inspection*)

- Para entender melhor, suponha que um aplicativo iniciou um acesso para transferência de arquivos entre um cliente e um servidor. Os pacotes de dados iniciais informam quais portas TCP serão usadas para esta tarefas. Se de repente o tráfego começar a fluir por uma porta não mencionada, o firewall pode então detectar esta ocorrência como uma anormalidade e efetuar o bloqueio.

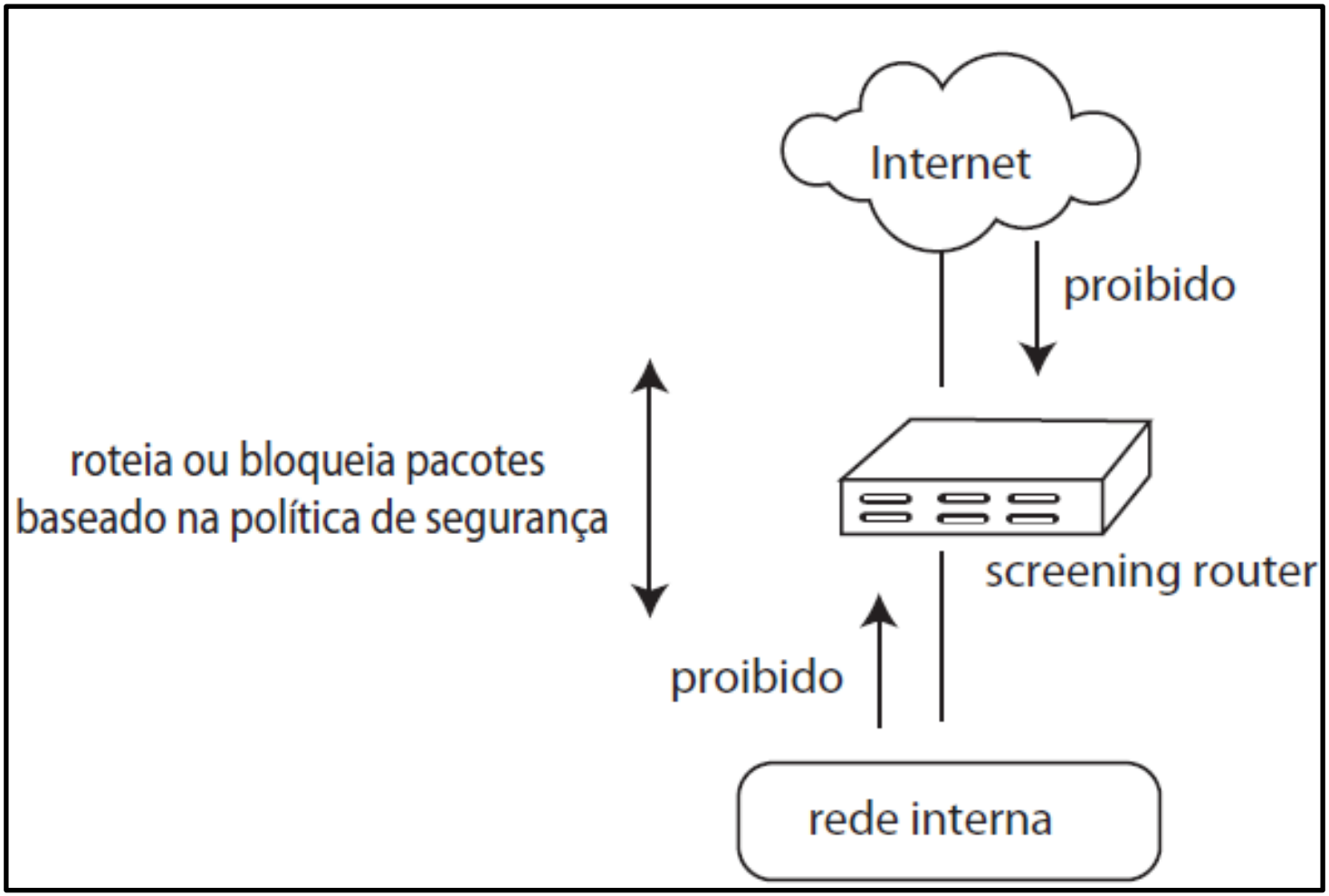
Arquitetura dos Firewalls

- A julgar pela variedade de **tipos**, os firewalls podem ser implementados de várias formas para atender às mais diversas necessidade. Este aspecto leva a outra característica importante do assunto: **arquitetura** de um firewall
- Arquitetura do **firewall** é a forma como é **projetado** e **implementado**
- Há, basicamente, três tipos de arquiteturas: *Single-Box*, *Dual-Homed Host*, *Screened Host* e *Screened Subnet*

Arquitetura dos Firewalls – *Single Box*

- Esta arquitetura tem como característica a utilização de um único objeto para executar as funcionalidades de firewall.
- Vantagem
  - a simplicidade e o barateamento de custo; e, como
- Desvantagem,
  - a vulnerabilidade (é o único ponto de defesa).

Arquitetura dos Firewalls – *Single Box*



Arquitetura dos Firewalls - *Dual-Homed Host*

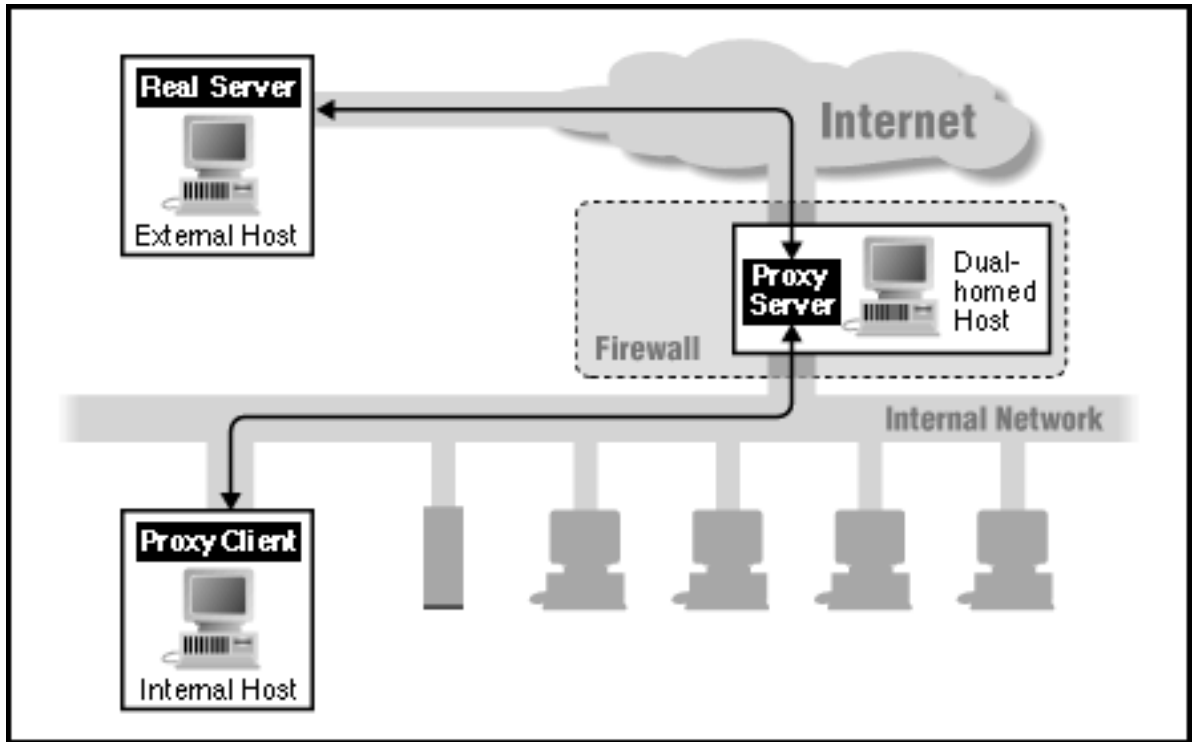
- Nesta arquitetura existe um computador chamado ***dual-homed host*** que fica entre uma rede interna e a rede externa – normalmente, a internet. O nome se deve ao fato de este host possuir ao menos duas interfaces de rede, uma para cada “lado”

- todo o tráfego passa por este firewall, não havendo acesso da rede interna para a rede externa (e vice-versa) diretamente

- Vantagem: há grande controle do tráfego

Arquitetura dos Firewalls - *Dual-Homed Host*

- **Desvantagem**: qualquer problema com o ***dual-homed*** – uma invasão, por exemplo – pode pôr em risco a segurança da rede ou mesmo paralisar o tráfego. Por esta razão, o seu uso pode não ser adequado em redes cujo acesso à internet é essencial
- Este tipo de arquitetura é bastante utilizado para firewalls do tipo proxy



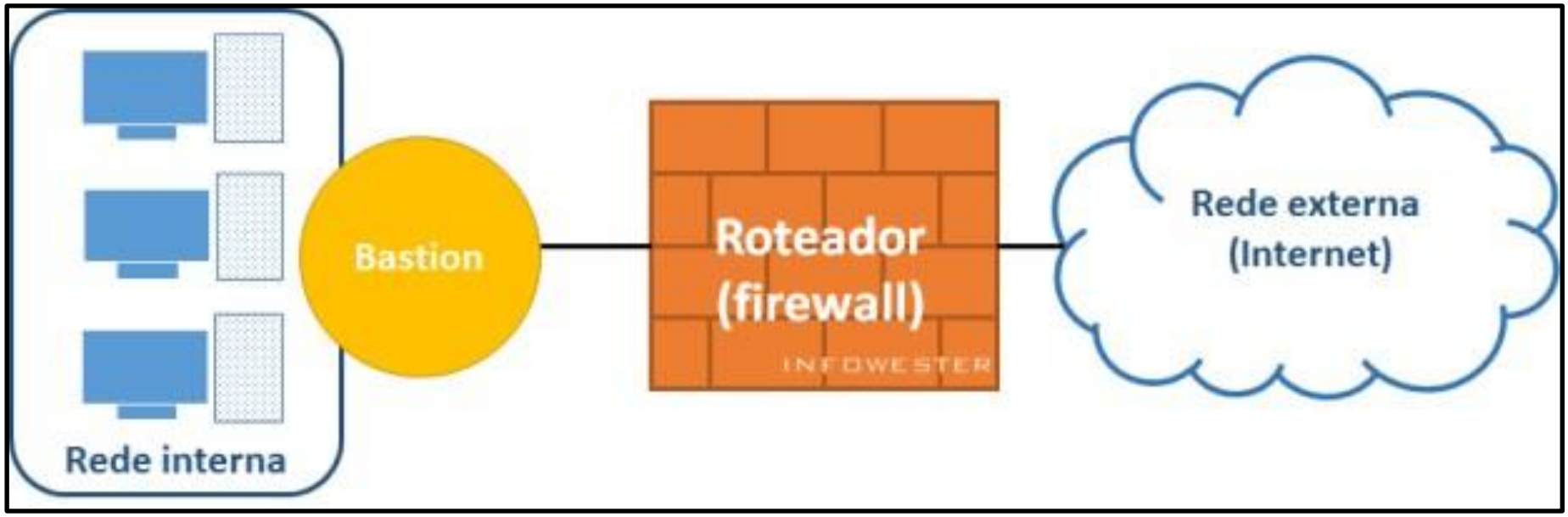
Arquitetura dos Firewalls - *Screened Host*

- Em vez de haver uma única máquina servindo de intermediadora entre a rede interna e a rede externa, há duas: uma que faz o papel de roteador (*screening router*) e outra chamada de ***bastion host***.

- O ***bastion host*** atua entre o roteador e a rede interna, não permitindo comunicação direta entre ambos os lados

- Então trata se de uma camada extra de segurança: a comunicação ocorre no sentido rede interna – *bastion host* – *screening router* – rede externa e vice-versa

Arquitetura dos Firewalls - *Screened Host*



Arquitetura dos Firewalls - *Screened Host*

- O roteador normalmente trabalha efetuando filtragem de pacotes, sendo os filtros configurados para redirecionar o tráfego ao *bastion host*. Este, por sua vez, pode decidir se determinadas conexões devem ser permitidas ou não, mesmo que tenham passado pelos filtros do roteador

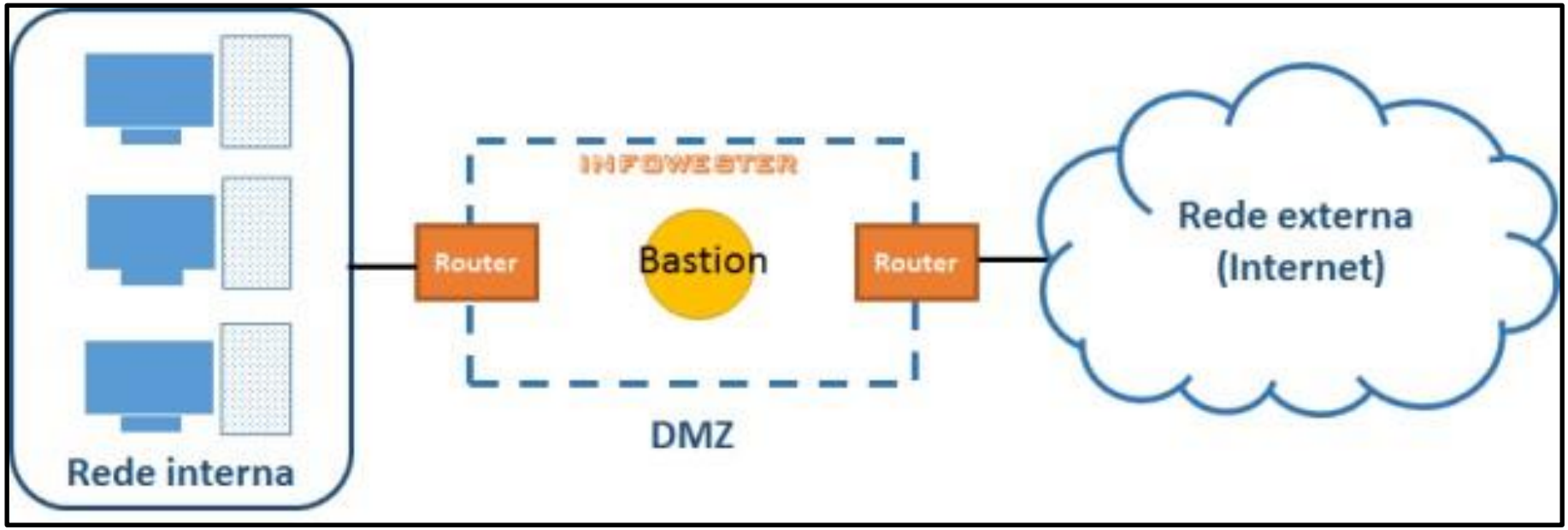
- **Ponto Crítico da Estrutura**: o *bastion host* precisa ser bem protegido, do contrário, colocará em risco a segurança da rede interna ou ainda poderá torná-la inacessível.

Arquitetura dos Firewalls - *Screened Subnet*

- A arquitetura *Screened Subnet* também conta com a figura do *bastion host*, mas este fica dentro de uma área isolada de nome interessante: a DMZ, sigla para *De-Militarized Zone* – Zona Desmilitarizada

- A DMZ, por sua vez, fica entre a rede interna e a rede externa. Acontece que, entre a rede interna e a DMZ há um roteador que normalmente trabalha com filtros de pacotes. Além disso, entre a DMZ e a rede externa há outro roteador do tipo

Arquitetura dos Firewalls - *Screened Subnet*

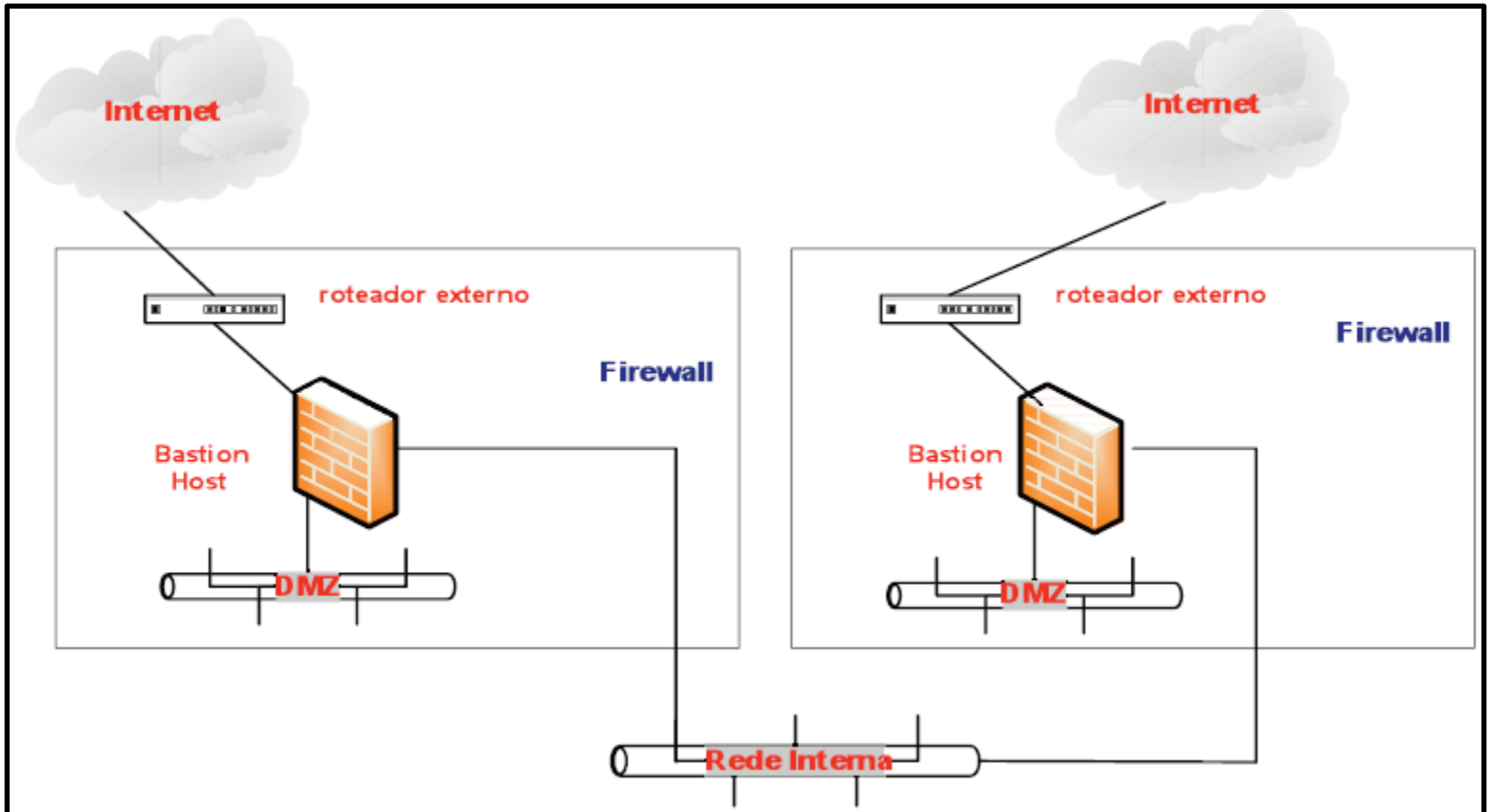


Arquitetura dos Firewalls - *Screened Subnet*

- Esta arquitetura se mostra bastante segura, uma vez que, caso o invasor passe pela primeiro roteador, terá ainda que lidar com a zona **desmilitarizada**.
- Esta inclusive pode ser configurada de diversas formas, com a implementação de proxies ou com a adição de mais ***bastion hosts*** para lidar com requisições específicas, por exemplo.
- O nível segurança e a flexibilidade de configuração fazem da ***Screened Subnet*** uma arquitetura normalmente mais complexa e, consequentemente, mais cara.

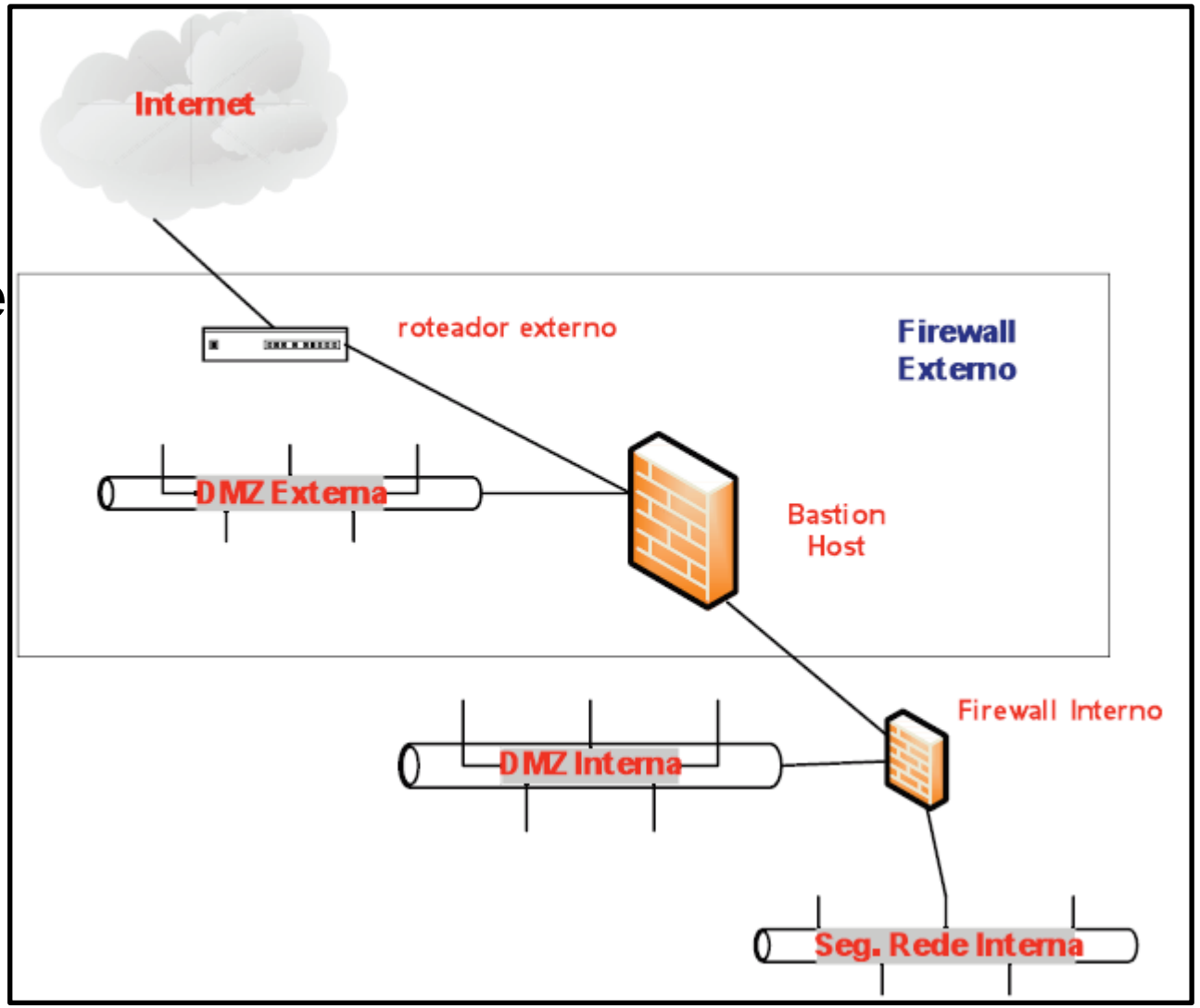
Arquitetura dos Firewalls - *Screened Subnet Independentes*

- Este tipo de arquitetura é apropriado em redes com uma forte necessidade de **redundância**, alta necessidade de segurança e faz uso de **vários serviços** da internet.



Arquitetura dos Firewalls - *Internos*

- A utilização de firewalls não é exclusiva para proteger a **rede interna** da **internet**.
- Pode-se, às vezes, necessitar **proteger as partes da rede interna** de outras partes.



Firewalls pessoais

- Há firewalls mais simples destinados a proteger o seu computador, seja ele um desktop, um laptop, um tablet, enfim. São os firewalls pessoais (ou domésticos), que DEVEM ser utilizados por qualquer pessoa

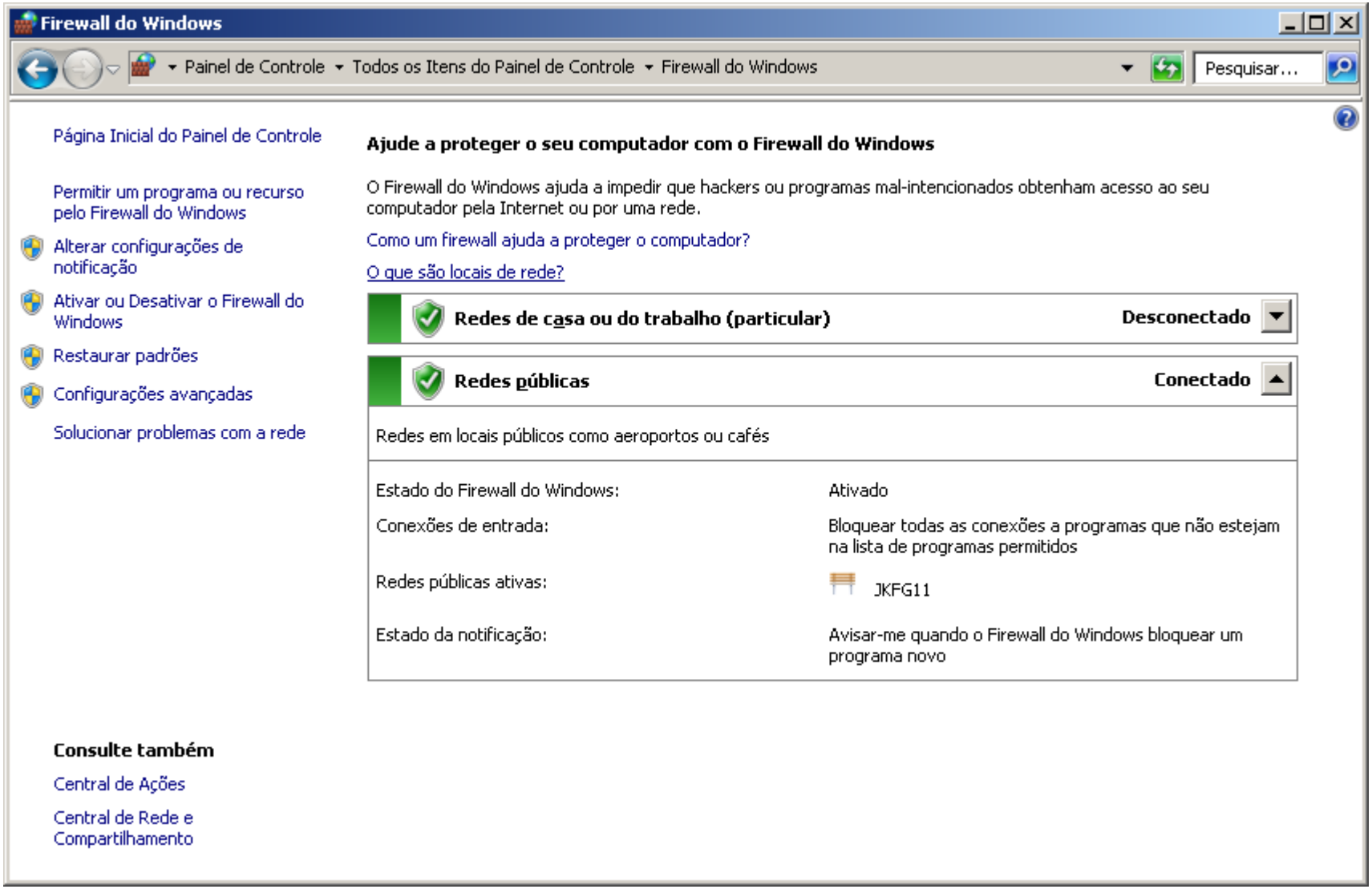
- Felizmente, sistemas operacionais atuais para uso doméstico ou em escritório costumam conter firewall interno por padrão, como é o caso de distribuições Linux, do Windows X ou do Mac OS X. Além disso, é comum desenvolvedores de antivírus oferecerem outras opções de proteção junto ao software, entre elas, um firewall.

Firewalls pessoais

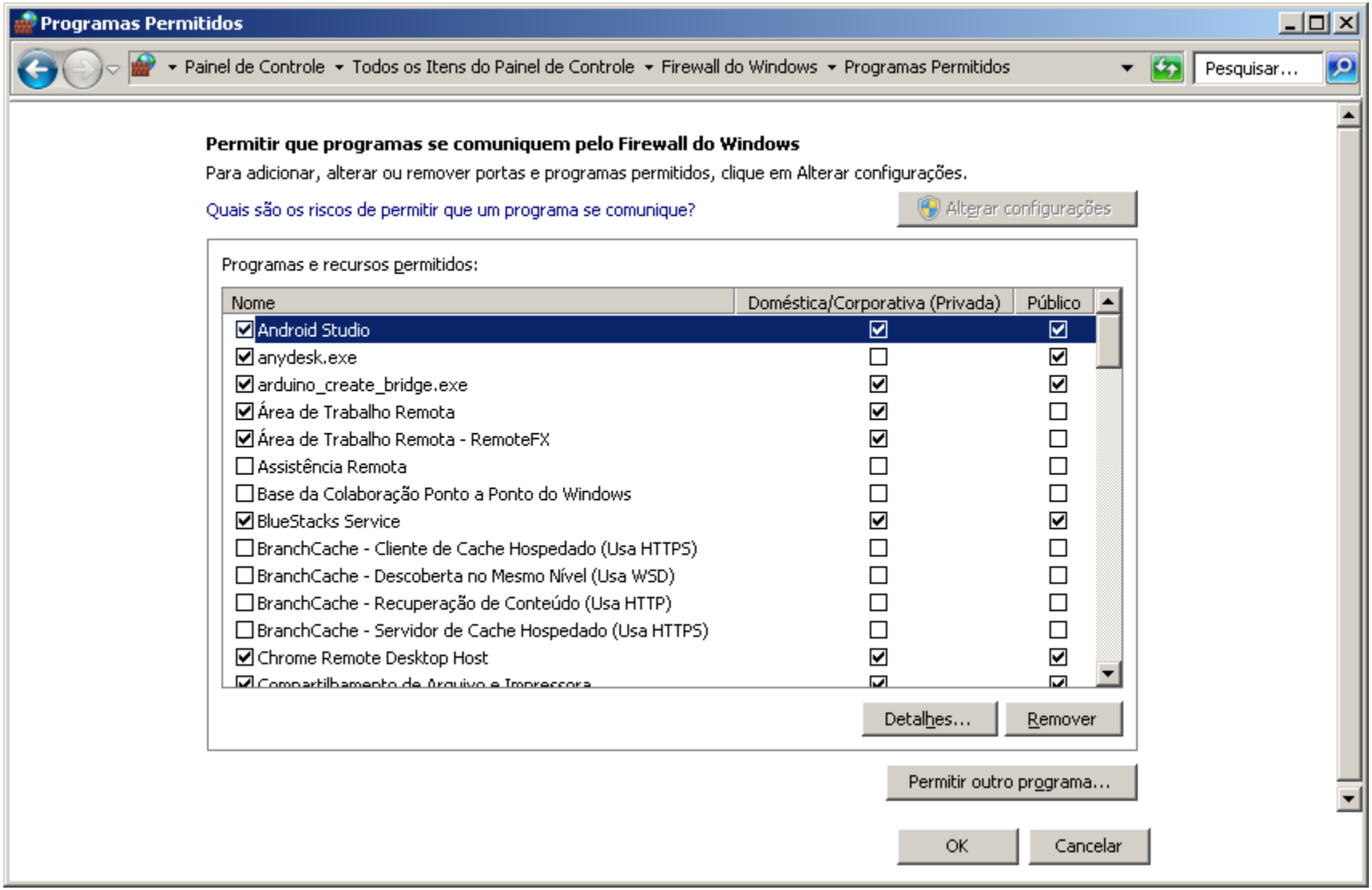
- Mas, para quem procura uma solução mais eficiente e que permita vários tipos de ajustes, é possível encontrar inúmeras opções, muitas delas gratuitas. Usuários de Windows, por exemplo, podem contar com o ZoneAlarm, com o Comodo, entre outros.

- Independente de qual seja o seu sistema operacional, vale a pena pesquisar por uma opção que possa atender às suas necessidades.

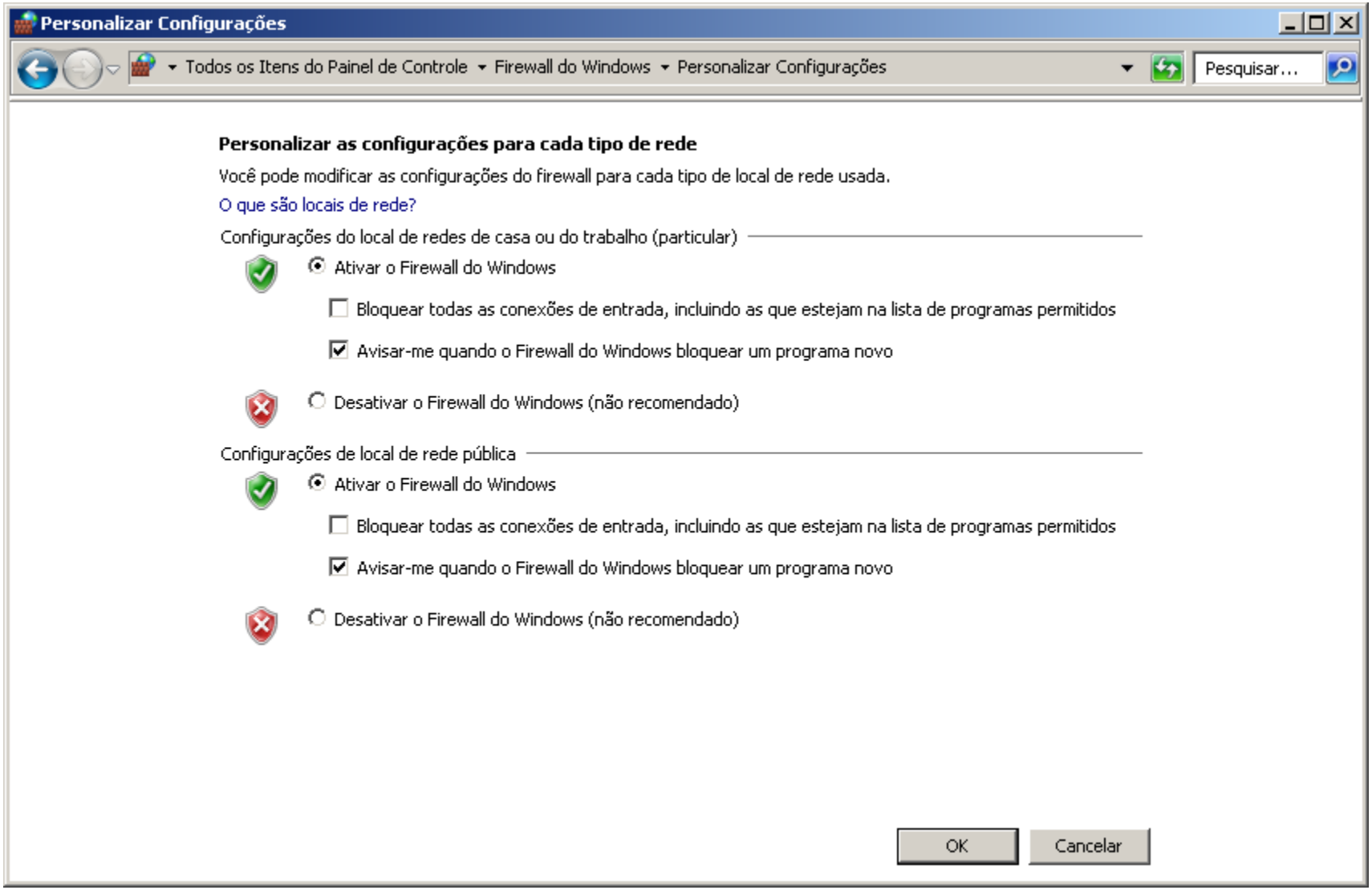
Firewall - Funcionamento



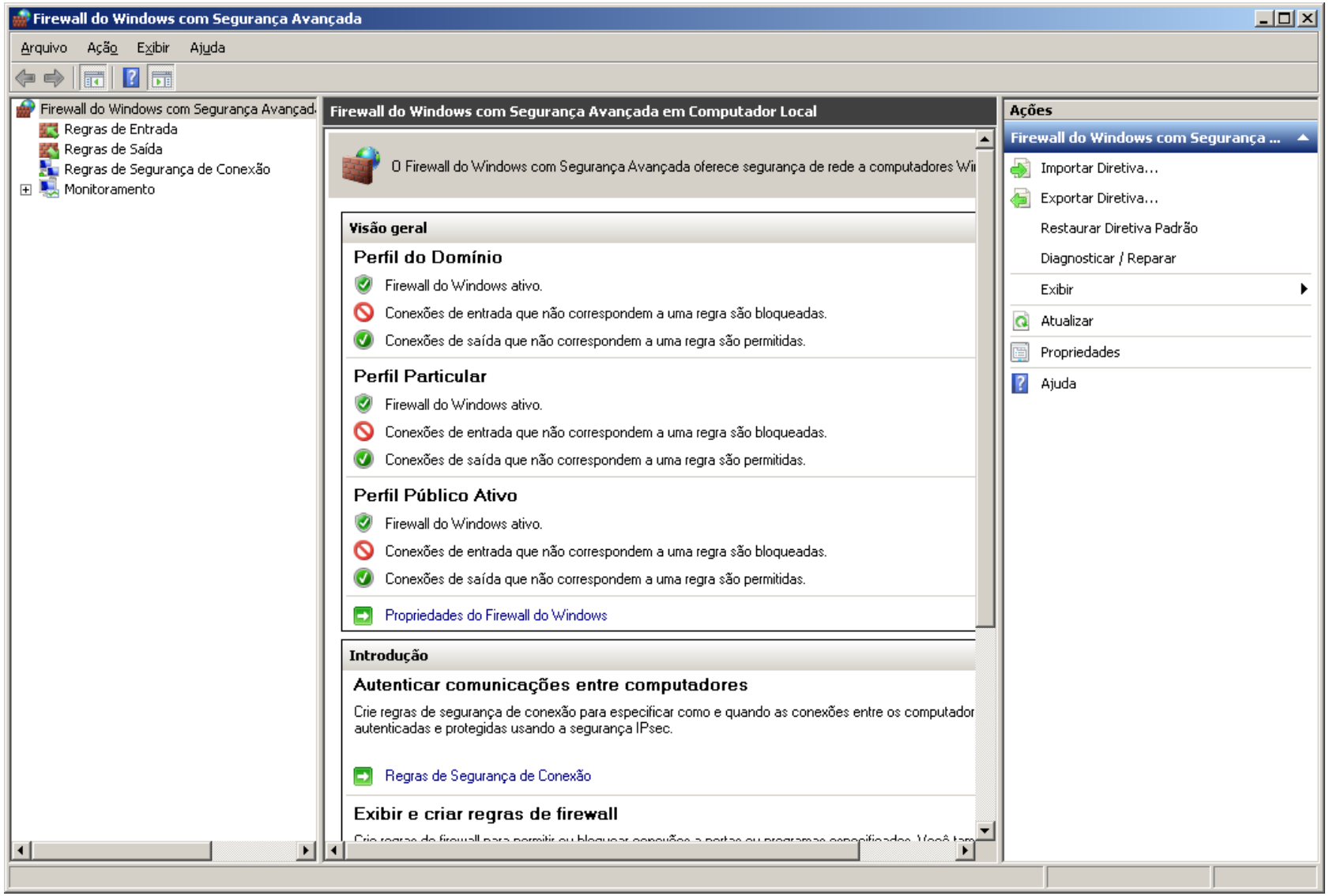
Firewall - Funcionamento



Firewall - Funcionamento



Firewall - Funcionamento



Firewalls de Hardware

- Já foi mencionado o fato de um firewall poder ser uma solução de software ou hardware.
- **ESTA INFORMAÇÃO NÃO ESTÁ INCORRETA**, mas é necessário um complemento:
- **O HARDWARE NADA MAIS É DO QUE UM EQUIPAMENTO COM UM SOFTWARE DE FIREWALL INSTALADO.**
- É possível encontrar, por exemplo, roteadores ou equipamentos semelhantes a estes que exercem a função em questão função. Neste caso, o objetivo normalmente é o de proteger uma rede com tráfego considerável ou com dados muito importantes

Firewalls de Hardware

- A vantagem de um **Firewall de hardware** é que o equipamento, por ser desenvolvido especificamente **para este fim**, é preparado para lidar com grandes volumes de dados e não está sujeito a vulnerabilidades que eventualmente podem ser encontrados em um servidor convencional (por conta de uma falha em outro software, por exemplo).

Protocolo TCP

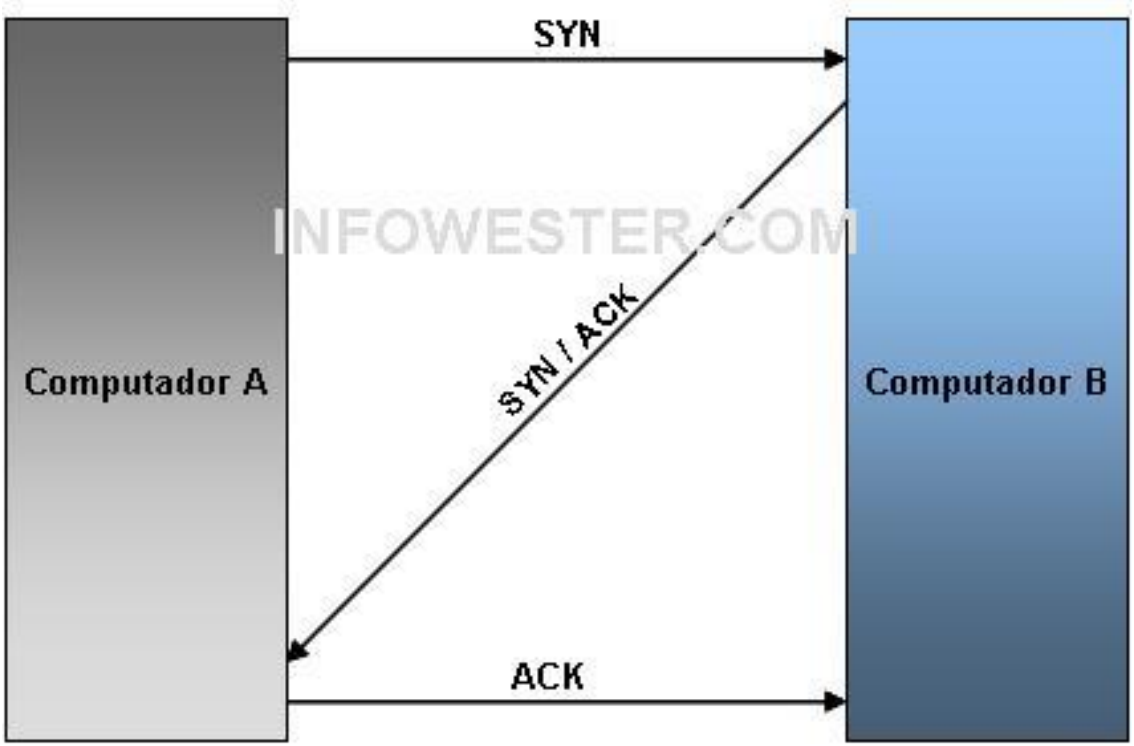
- A comunicação pela internet é feita, basicamente, através de protocolos, sendo o **TCP** (*Transmission Control Protocol*).
- **TCP** está incluído no conjunto de protocolos que formam o TCP/IP, a base de comunicação via dados de toda a internet.

Protocolo TCP

- Baseado em conexões.
- Para um computador **cliente** iniciar uma "conversa" com um servidor, é necessário enviar um sinal denominado SYN para este último.
- O **servidor** então responde enviando um sinal SYN combinado com um sinal de nome ACK para confirmar a conexão.
- O **cliente** responde com outro sinal ACK, fazendo com que a conexão esteja estabelecida e pronta para a troca de dados.

Protocolo TCP

- Por ser feita em três transmissões, esse processo é conhecimento como *three-way handshake* (algo como triplo aperto de mãos).



https://www.infowester.com/portastcpudp.php

Protocolo UDP

- O UDP (*User Datagram Protocol*) é tido como um protocolo "irmão" do TCP, mas é mais simples e também menos confiável.
- O funcionamento do TCP é, como já dito, baseado em conexões, o que não ocorre com o UDP.
- Como consequência, não há procedimentos de verificação no envio e recebimento de dados (todavia, pode haver checagem de integridade) e se algum pacote não for recebido, o computador de destino não faz uma nova solicitação, como acontece com o TCP.
- Tudo isso faz do UDP um pouco mais rápido, porém inutilizável em certas aplicações.

Portas TCP e portas UDP

- Suponha que, neste momento, você esteja usando um navegador de internet, um cliente de e-mail e um software de comunicação instantânea.
- Todas essas aplicações fazem uso da sua conexão à internet, mas como o computador faz para saber quais os dados que pertencem a cada programa?
- Simples, pelo número da **porta** que cada um utiliza.
- Por exemplo, se você está usando um programa de FTP (*File Transfer Protocol*), a conexão à internet é feita pela porta TCP 21, que é uma porta convencionada a este protocolo.
- Se estiver baixando arquivos pelo BitTorrent, uma das portas que vão de 6881 à 6889 estará sendo utilizada para tal atividade.

Portas mais comuns

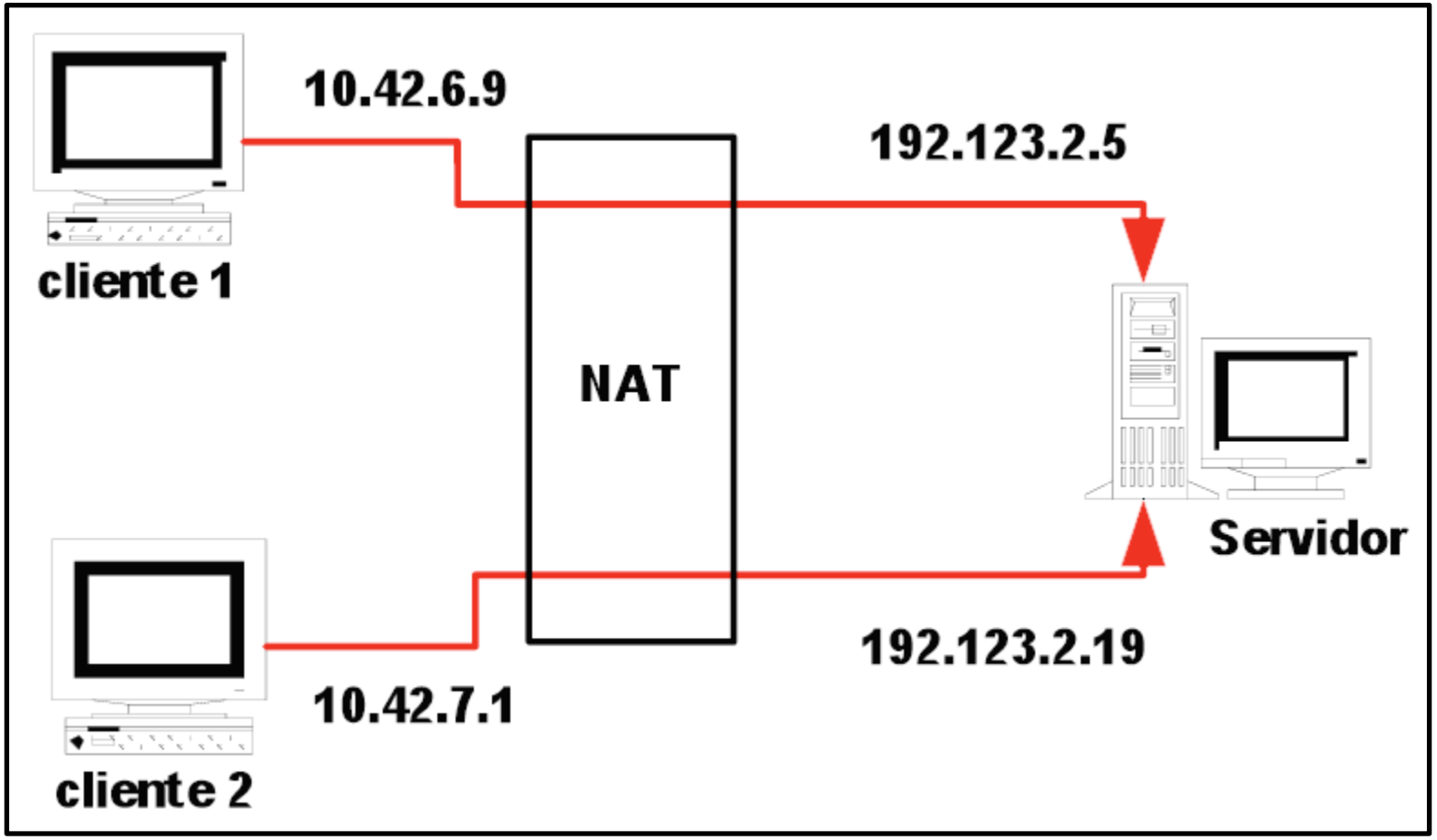
- É possível usar 65536 portas TCP e UDP, começando em 1. Tanto no protocolo TCP como no UDP, é comum o uso das portas de 1 a 1024, já que a aplicação destas é padronizada pela IANA (*Internet Assigned Numbers Authority*).
- De acordo com essa entidade as portas TCP mais utilizadas:
  - 21 - FTP;
  - 23 - Telnet;
  - 25 - SMTP;
  - 80 - HTTP;
  - 110 - POP3;
  - 143 - IMAP;
  - 443 - HTTPS.

https://pt.wikipedia.org/wiki/Lista_de_portas_dos_protocolos_TCP_e_UDP

NAT – *Network Address Translation*

- O NAT admite que uma rede utilize um **conjunto de endereços internos** e um **conjunto diferente de endereços**, quando negociando com redes externas.
- O **NAT**, por ele mesmo, não provê segurança, mas ajuda a **esconder o layout da rede interna** e força que todas as conexões sejam realizadas via um **único ponto de passagem(Firewall)**.

NAT – *Network Address Translation*



NAT – *Network Address Translation*

- O **NAT** pode fazer uso de diferentes formas para mapear os endereços internos em endereços externos, e vice-versa.
- Logo, o **NAT** possibilita:
  - alocar um endereço externo para cada endereço interno e sempre aplicar a mesma regra. Essa é uma medida temporária, utilizada por sites que têm o seu espaço de endereçamento ilegalmente utilizado;
  - alocar, de forma dinâmica, um endereço externo a cada vez que uma máquina interna inicia uma conexão, sem modificar o número das portas. Limita-se o número de máquinas internas que podem simultaneamente acessar a internet ao número de endereços externos disponíveis;
  - criar um mapeamento entre os endereços internos e os externos;
  - alocar dinamicamente o par de porta e o endereço externo a cada conexão iniciada por uma máquina interna.

IPTABLES

- Não é essencialmente um **firewall**, mas um programa que, por meio de seus módulos, possibilita ao usuário configurar o kernel Linux e o conjunto de regras do filtro de pacotes — função típica do firewall.

- Na prática, o administrador de sistemas tem de gerenciar quatro tabelas (filter, NAT, mangle e security) com funções distintas e, com isso, aplicar as regras desejadas. Como a interação ocorre quase diretamente com o kernel, praticamente não há limites quanto à aplicação de regras via **iptables**.

IPTABLES

- O **iptables** é um programa escrito em C, utilizado como ferramenta que configura regras para o protocolo de internet IPv4 na tabela de filtragem de pacotes, utilizando os módulos e framework do kernel Linux (versão 2.3.15 ou posteiro).
- As configurações de **firewall** feitas ficarão guardadas no kernel, logo serão perdidas quando o sistema for reiniciado.
- O **iptables-save** e **iptables-restore** ficam responsáveis por salvar as configurações e restaurá-las.

IPTABLES

- Organiza suas regras em uma estrutura que contém tabelas e cadeias. As tabelas são um agrupamento de cadeias em um nível mais alto, e determinam grosso modo o escopo das regras que serão criadas.
- Possui diversas tabelas ou listas de regras:
  - **filter** – Tabela padrão para manipular pacotes de rede, usada para configurar políticas para o tráfego uqe entra, atravessa ou sai do computador.
  - **nat** – Usada para alterar pacotes que criam uma nova conexão, e para redirecionar conexões para NAT..
  - **mangle** – Usada para tipos específicos de alteração de pacotes, como a modificação de opções do cabeçalho IP de um pacote..
  - **raw** – Marca pacotes que não devem ser manipulados pelo sistema de rastreamento de conexões.

IPTABLES

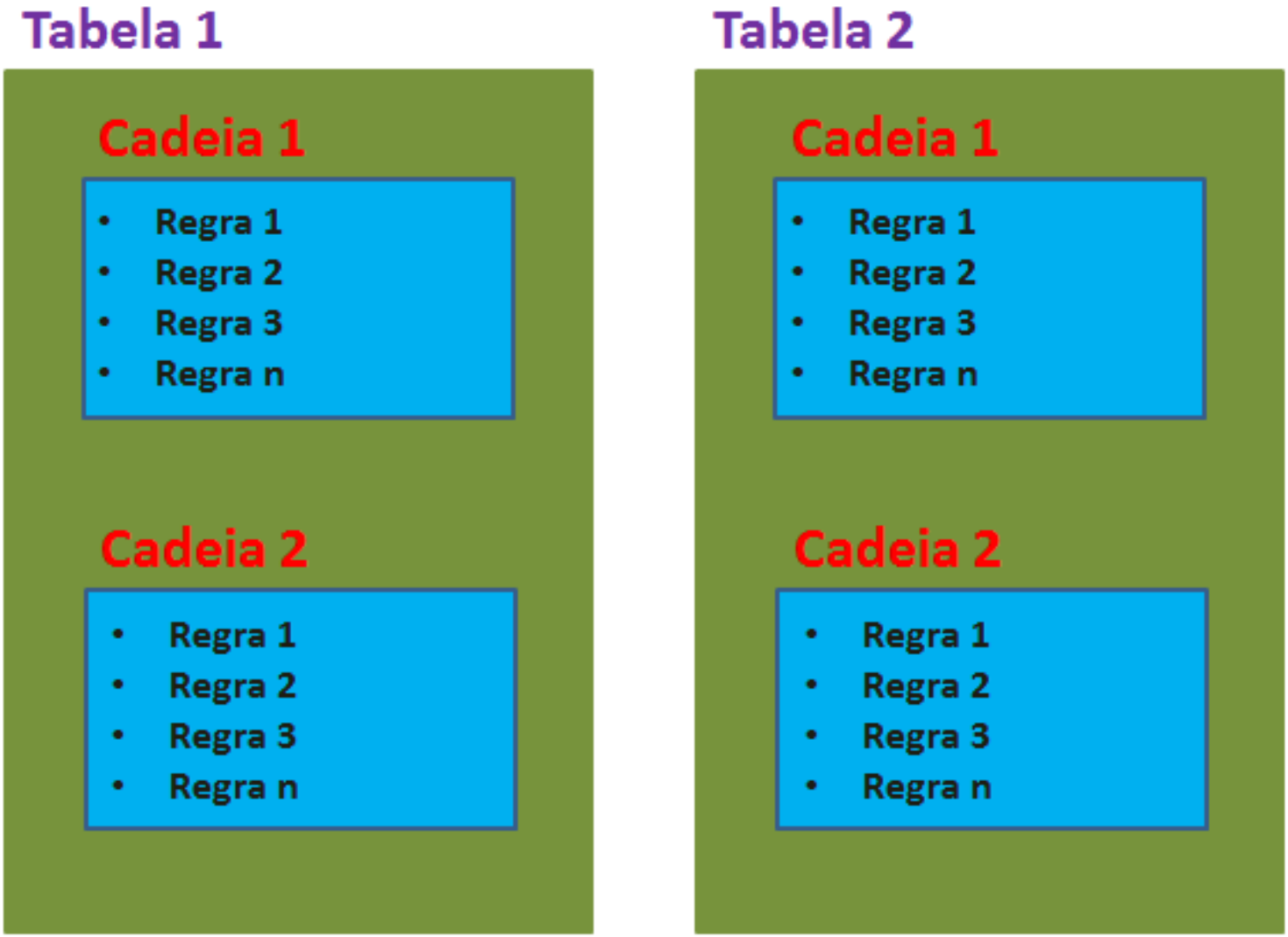


Tabela 1
Cadeia 1
Regra 1
Regra 2
Regra 3
Regra n
Cadeia 2
Regra 1
Regra 2
Regra 3
Regra n
Tabela 2
Cadeia 1
Regra 1
Regra 2
Regra 3
Regra n
Cadeia 2
Regra 1
Regra 2
Regra 3
Regra n

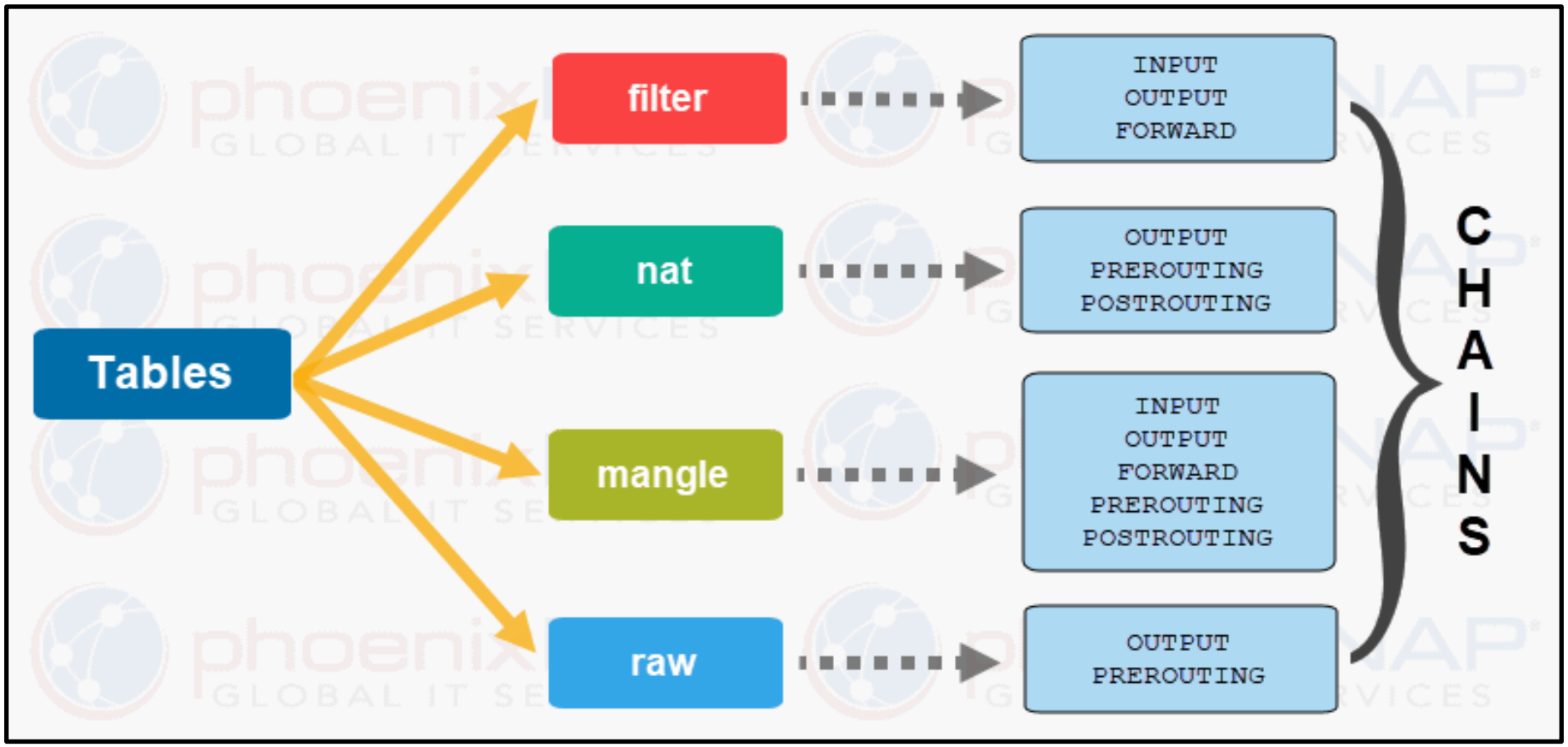
IPTABLES

- As tabelas podem possuir as cadeias:
  - Tabela FIlter: Cadeias INPUT, OUTPUT e FORWARD
  - Tabela NAT: Cadeias PREROUTING, OUTPUT, POSTROUTING
  - Tabela Mangle: Cadeias PREROUTING, OUTPUT, POSTROUTING, INPUT e FORWARD
  - Tabela raw: Cadeias PREROUTING e OUTPUT
  - Tabela security – Usada para regras de rede MAC (Mandatory Access Control)

IPTABLES

- Cadeias
  - As regras são organizadas em grupos denominados cadeias (**chains**), que por sua vez ficam contidas nas tabelas. Uma cadeia é então um conjunto de regras usadas para verificar a correspondência com um pacote – de forma sequencial.
  - Um pacote é verificado junto às regras na ***chain***, e se não há correspondência, a próxima regra na ordem é verificada. Quando um pacote corresponde a uma regra na cadeia, a ação associada a essa regra é executada e as regras restantes não são verificadas contra esse pacote. Caso nenhuma regra corresponda ao pacote, a regra padrão (*policy*) será aplicada.

IPTABLES


Tables
filter
nat
mangle
raw
INPUT
OUTPUT
FORWARD
OUTPUT
PREROUTING
POSTROUTING
INPUT
OUTPUT
FORWARD
PREROUTING
POSTROUTING
OUTPUT
PREROUTING
CHAINS

IPTABLES

- Algumas aplicações do iptables:
  - Construir firewalls de Internet baseados em filtragem de pacotes “*stateless*” e “*stateful*”
  - Usar NAT e *masquerading*(disfarce) para compartilhamento de Internet com uma rede local
  - Usar NAT para implementar proxies transparentes
  - Realizar manipulação de pacotes adicional (*mangling*/mutilar), como alterar bits no cabeçalho IP
  - Monitorar o volume de tráfego de rede
  - Realizar Encaminhamento de Portas (que é um tipo de DNAT)
  - Balanceamento de carga de rede.

IP Spoofing

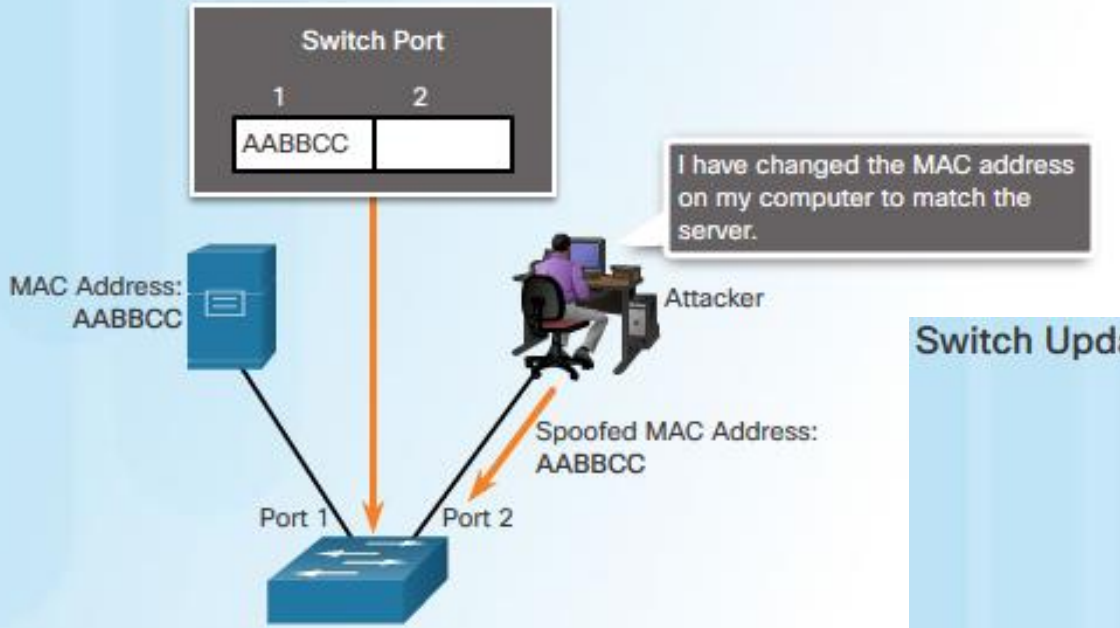
- O Ataque de Spoofing utiliza conceitos de confiança e autenticação entre máquinas
- Não é exatamente uma forma de ataque, mas uma técnica que é utilizada na grande maioria dos ataques para esconder a identidade do atacante

Manipulação direta do cabeçalho do pacote IP

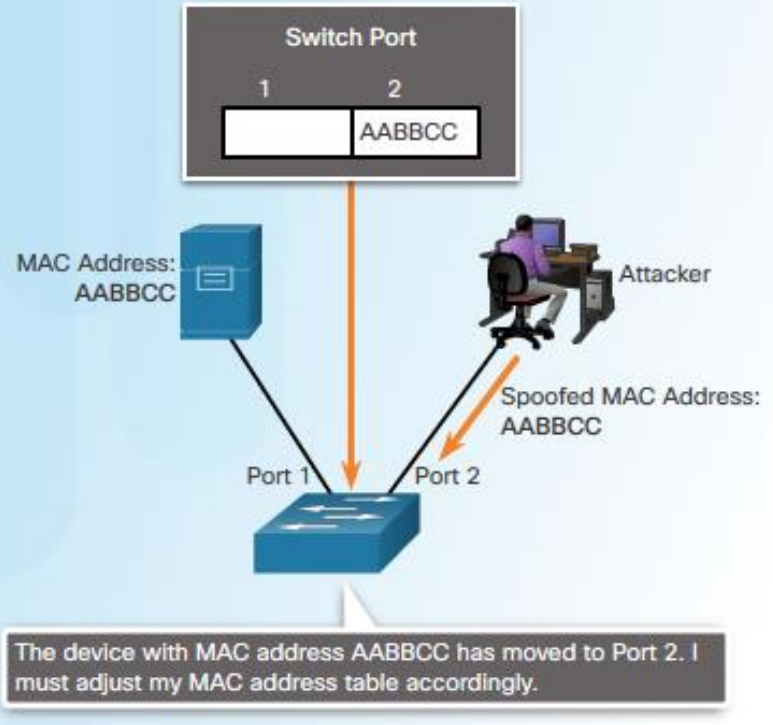
IP Spoofing

- **Todos que trabalham com Firewall devem saber!**
- Regras Anti-Spoofing:
  - **Apenas devem sair** de sua rede local pacotes que possuam endereços IP de origem de sua organização
  - **Não devem entrar** na sua rede local pacotes com endereços IP de origem de sua organização (foram falsificados)

Attacker Spoofs a Server's MAC Address



Switch Updates CAM Table with Spoofed Address



Limitações dos Firewalls

Resumindo, podemos mencionar as seguintes limitações:

- Um firewall pode oferecer a segurança desejada, mas comprometer o desempenho da rede (ou mesmo de um computador). Esta situação pode gerar mais gastos para uma ampliação de infraestrutura capaz de superar o problema;
- A verificação de políticas tem que ser revista periodicamente para não prejudicar o funcionamento de novos serviços;
- Novos serviços ou protocolos podem não ser devidamente tratados por proxies já implementados;
- Um firewall pode não ser capaz de impedir uma atividade maliciosa que se origina e se destina à rede interna;

O que um Firewall faz e não faz?

- O que o firewall faz?
  - Ele impede que seu computador seja invadido;
  - Não permite que dados indesejáveis entrem em uma máquina;
  - O firewall bloqueia o envio de dados originários de uma máquina que não estejam especificados nas configurações;
- O que o firewall não faz?
  - O firewall não protege as máquinas contra programas baixados pelos usuários;
  - Não impede que programas de e-mail baixem spam nas máquinas;
  - Não impede que o usuário crie exceções errôneas que podem colocar o computador em risco.

https://www.tecmundo.com.br/seguranca/3329-como-funciona-o-firewall-.htm

Atividade

- Vamos responder as 30 questões a seguir!
- Para cada questão terá um tempo para ser respondido.
- Marque duas respostas para a questão.
  - A primeira resposta deve ser marcada nos 30 segundos iniciais. Esta resposta é definida com uma primeira avaliação com base no foi apresentado na aula.
  - Para a segunda resposta pesquise no material e na web para responder.
  - Tente acertar o maior número de respostas na primeira tentativa.

Questão 1

- (FUNDANTEC, 2020) É um dispositivo de uma rede de computadores, na forma de um programa (software) ou de equipamento físico (hardware), que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede, geralmente associados a redes TCP/IP. O texto fala de um:

A vírus.

B switch.

C firewall.

D hub.

E navegador.

Questão 2

- (IBADE, 2019) O acesso a uma rede privada necessita de proteção e garantia de origem. Uma ferramenta que dá proteção a redes de computadores impedindo acessos não autorizados é:

A Criptografia.

B Anti-Vírus.

C Hub.

D FireWall.

E Band Switch.

Questão 3

- (CESPE/CEBRASPE, 2006) Julgue o item subsequente, referente a conceitos e aplicabilidade de mecanismos de segurança.

- Um firewall é um dispositivo que permite realizar a segmentação de uma rede local e provê características de segurança puramente física.

A Certo

B Errado

Questão 4

- (IBADE, 2019)As redes de computadores, do tipo WAN, que se utilizam da internet, são alvo frequente de tentativas de invasão e necessitam de proteção. Para proteção contra invasores e restrição de acesso apenas aos computadores autorizados, qual das ferramentas abaixo é indicada ?

A Anti-Vírus

B Criptografia

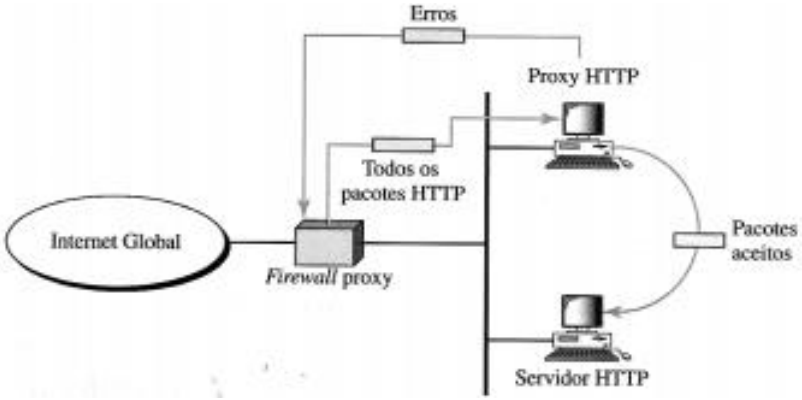
C Certificado Digital

D Validador Eletrônico

E FireWall

Questão 5

- (FGV, 2012)O firewall de filtragem de pacotes se baseia nas informações disponíveis nos cabeçalhos da camada de rede e de transporte IP. Quando a filtragem de pacotes não é viável, a solução é instalar o firewall proxy, que fica posicionado entre o computador-cliente e o da empresa, conforme indicado na figura abaixo.



- Um firewall proxy faz a filtragem na seguinte camada do modelo OSI/ISO:

A Rede B Física C Aplicação

D Transporte E Apresentação

Questão 6

- (TRE SP 2013) Sobre os firewalls é correto afirmar:

A Pode autorizar ou negar acesso, mas não pode registrar tudo o que está passando por ele.

BOs firewalls de proxy examinam os pacotes superficialmente, não verificando seu conteúdo. Isso os torna mais rápidos porém, menos eficientes.

CO tráfego interno na mesma subrede de uma LAN, ou seja, o que não vai para uma rede externa, sempre é tratado pelo firewall, pois todo o tráfego passa por ele.

D Os firewalls de filtro de pacotes trabalham com uma lista de controle de acesso que é verificada antes de um pacote ser encaminhado para a rede interna. A lista relaciona o tráfego que é permitido e o que deve ser bloqueado.

E Os firewalls de filtro de pacotes são rápidos porque a inspeção é feita em vários pacotes por vez. Eles escondem automaticamente os endereços de rede e não requerem muitos testes para verificar suas funcionalidades.

Questão 7

- Em relação a firewalls, analise as afirmativas abaixo:

I. Firewalls protegem contra a infecção por vírus, analisando o conteúdo de todos os arquivos, mensagens e e-mails.

II. Uma das fraquezas de firewalls é a impossibilidade da inclusão de auditorias e alarmes nas suas configurações.

III. Existem diferentes tipos de firewalls, como o filtro de pacotes e o proxy, por exemplo.

Está correto somente o que se afirma em:

A I;

B II;

C III;

D I e II;

E II e III.

Questão 8

- (TRT 8, 2014) Assinale a opção em que são apresentadas as características genéricas de um firewall.

A Validar select executado por uma aplicação web em um banco de dados DB2.

B Permitir acesso a um sistema e a análise de ataques por meio de estatísticas de anomalia relacionadas aos comportamentos dos usuários.

C Analisar switches defeituosos na rede de computadores.

D Capacidade para concentrar e filtrar os acessos dial-in à rede e suportar a funcionalidade de proxy para serviços FTP.

E Criptografar os dados de uma aplicação de intranet na rede interna.

Questão 9

- (CESPE, 2015) Após uma auditoria de segurança na rede de comunicação de determinado órgão do governo, constatou-se que a parte de navegação na Internet desse órgão não possuía nenhum tipo de filtro de pacotes. Por isso, o auditor solicitou a instalação de um firewall Linux IPTABLES e um proxy SQUID entre as estações da rede e a Internet.
- Considerando essa situação hipotética, julgue o item que se segue, relativo a firewall e proxy.
- O firewall IPTABLES permite o uso de filtro de pacotes, de forma a controlar o fluxo de dados entre a rede local e a Internet, interferindo em situações normais até a camada de transporte do modelo TCP/IP.

A Certo

B Errado

Questão 10

- (ANTT 2013) Acerca do sistema operacional Windows, julgue os itens subsequentes. O perfil de firewall definido como private é aplicado ao computador em qualquer rede que se conecte, quando um domínio Active Directory está indisponível.

A Certo

B Errado

Questão 11

- (CONSULPLAN 2019) Para realizar a manutenção em uma máquina, devido a alguns fatores, deve-se fazer acesso remoto a determinada estação de trabalho, que usa o Sistema Operacional Windows 10, Configuração Local, Idioma Português-Brasil. O comando a ser utilizado é o TELNET, sendo necessário saber se a porta de comunicação desse protocolo está aberta no Firewall. Esta porta está apresentada em:

A 20

B 21

C 22

D 23

Questão 12

- (ANTT, 2013) Julgue os itens subsequentes com relação a ataques a redes de computadores, prevenção e tratamento de incidentes. Firewall pode ser utilizado para proteger um computador contra acessos não autorizados advindos da Internet. Se estiver bem configurado, este tipo de proteção possibilita a identificação das origens destas tentativas e interrompe a comunicação entre um invasor e um código malicioso já instalado, entre outras ações.

A Certo

B Errado

Questão 13

- (TRE SP 2013) Sobre os firewalls é correto afirmar:

A Pode autorizar ou negar acesso, mas não pode registrar tudo o que está passando por ele.

B Os firewalls de proxy examinam os pacotes superficialmente, não verificando seu conteúdo. Isso os torna mais rápidos porém, menos eficientes.

C O tráfego interno na mesma subrede de uma LAN, ou seja, o que não vai para uma rede externa, sempre é tratado pelo firewall, pois todo o tráfego passa por ele.

D Os firewalls de filtro de pacotes trabalham com uma lista de controle de acesso que é verificada antes de um pacote ser encaminhado para a rede interna. A lista relaciona o tráfego que é permitido e o que deve ser bloqueado.

E Os firewalls de filtro de pacotes são rápidos porque a inspeção é feita em vários pacotes por vez. Eles escondem automaticamente os endereços de rede e não requerem muitos testes para verificar suas funcionalidades.

Questão 14

- As ameaças também estão cada vez mais presentes no mundo virtual, os usuários conscientes devem saber evitar que seu computador seja atacado, porém alguns cuidados são fundamentais. Assinale a alternativa que define a função do Firewall que é um dispositivo de segurança que pode ser utilizado nessa proteção.

A Firewall tem objetivo de controlar o acesso a rede de computadores, e todo o tráfego deve passar por ele.

B Firewall é configuração que deve ser realizada quando equipamentos falham no acesso à internet por motivo de hardware ou software.

C Firewall é um software específico de proteção as redes sociais, pois evita o furto de dados e o acesso indevido a dados pessoais nas redes.

D Firewall, inibe o acesso indevido a conta bancária e consequentemente a realização de transações indesejadas.

Questão 15

- (AOCP, 2013 COREN-SC)Um firewall é responsável por filtrar pacotes recebidos e enviados a uma rede. Como é feita esta análise?

A O cabeçalho do pacote é analisado e liberado ou bloqueado com base em regras pré-definidas.

B O firewall libera ou bloqueia um pacote apenas verificando sua origem.

C O cabeçalho do pacote é analisado e o pacote é retido até que o administrador da rede o libere.

D O pacote é analisado e são corrigidos possíveis problemas nele pelo firewall.

E É realizada uma busca em um banco de dados mundial por possíveis falhas no pacote.

Questão 16

- (PRODEB)Um ponto muito importante referente à rede de computadores é a questão do firewall. A respeito do assunto, analise as assertivas e assinale a alternativa que aponta as corretas.

I. Aplicações com a função de firewall já são parte integrante de qualquer sistema operacional moderno, garantindo a segurança do PC desde o momento em que ele é ligado pela primeira vez.

II. Os firewalls trabalham usando regras de segurança, fazendo com que os pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final.

III. É bastante comum empresas usarem computadores específicos que agem como um "guardião" de uma rede, filtrando todo o trânsito de dados entre os PCs locais e um ambiente mais hostil, como a internet.

IV. O firewall controla o acesso ao meio em redes Ethernet e minimiza o problema de colisão entre pacotes

A Apenas I e IV.

B Apenas I, II e III.

C Apenas I e III

D Apenas II e IV

E Apenas III e IV

Questão 17

- (VUNESP, 2016)O administrador de uma rede local de computadores deseja bloquear os acessos para o serviço FTP em um Firewall do tipo filtragem de pacotes. Para isso, ele deve configurar o Firewall para bloquear os acessos pela Porta TCP de número

A 21.

B 23.

C 53.

D 110.

E 161.

Questão 18

- (INSTITUTO AOCP, 2019) A função básica de um firewall em um servidor é bloquear o acesso a portas que não estão em uso, evitando, assim, a exposição de serviços vulneráveis ou que não devem receber conexões por parte da internet. Sobre firewall, assinale a alternativa correta.

A Quando se configura um firewall, não é preciso se preocupar com portas UDP e TCP, uma vez que ele libera ou bloqueia as portas dos dois protocolos automaticamente.

B O firewall não pode ser implementado no sistema operacional e deve ser adquirido um equipamento físico de firewall.

C O Nagios é um exemplo de firewall que pode ser configurado através do sistema operacional Linux.

D Em um firewall, não há como bloquear pacotes ICMP.

E Ao configurar o firewall, é importante prestar atenção em relação ao uso do TCP ou do UDP, já que alguns protocolos utilizam uma combinação de portas TCP e UDP, como o Samba, que utiliza um total de quatro portas: 137 UDP, 138 UDP, 139 TCP e 445 TCP.

Questão 19

- (INSTITUTO AOCP, 2019)Um firewall de aplicativo proxy também pode ser referido como um gateway de aplicativo. Nesse cenário, o gateway se comporta como um intérprete, mediando as requisições entre os clientes e a rede externa. Assinale a alternativa que apresenta uma característica de um proxy.

A Bloqueia hosts com base no protocolo e número de porta de origem e destino.

B Analisa a camada de rede, tornando possível a filtragem de pacotes.

C Impede o tunelamento IP na rede.

D Consiste em um sistema de controle de acesso proprietário ou não que necessita de hardware exclusivo.

E O Firebase é um software que pode ser considerado um gateway de aplicativo.

Questão 20

- (COPESE/UFPI, 2020) Sobre o conceito, uso e configuração de um firewall, marque a opção INCORRETA.

A Pode ser uma implementação de hardware ou de software.

B Permite aplicar uma política de segurança a um determinado ponto da rede a qual está controlando o fluxo de pacotes.

C No firewall que implementa a filtragem estática, os dados são bloqueados ou liberados meramente com base nas regras, não importando a ligação que cada pacote tem com outro.

D Uma de suas funções também é impedir as colisões de pacotes, melhorando desempenho da rede.

E Um gateway de aplicativo de proxy é um recurso do firewall que combina o controle de acesso com a funcionalidade da camada superior atuando como um intermediário entre dois hosts que desejam se comunicar uns com os outros, nunca permitindo uma conexão direta entre eles.

Questão 21

- (COPESE UFT, 2012 -)Em relação à arquitetura de firewall, a preocupação reside na disposição dos equipamentos que compõem uma rede de computadores e o próprio firewall. Considere a separação entre a rede interna da organização da rede externa, que pode ser a internet, por meio da utilização de uma máquina que contenha duas interfaces de rede. Essa disposição consiste em uma arquitetura de firewall do tipo:

A Screened Host

B Dual-Homed Host

C Screened Subnet

D Screened-Homed

E Dual-Homed Subnet

Questão 22

- (CESPE/CEBRASPE, 2010)Um firewall tem três interfaces, conectadas da seguinte forma: uma à rede externa; outra à rede interna; e a terceira a uma DMZ. Nessa situação, considerando que o firewall registre todas as suas ações referentes ao exame do tráfego, julgue o item seguinte.

- A presença de vários registros idênticos referentes a um mesmo fluxo de tráfego é consistente com um firewall que tem por base a inspeção de pacotes.

A Certo

B Errado

Questão 23

- (UFCG, 2019)Um firewall é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

Analise as afirmativas abaixo:

I - Um firewall pode ser um hardware, software ou ambos.

II – Um firewall com inspeção de estado permite ou bloqueia tráfego de acordo com o estado, a porta e o protocolo.

III - Um firewall de proxy funciona como a passagem de uma rede para outra de uma aplicação específica, filtrando as mensagens, mascarando o endereço IP e limitando os tipos de tráfego.

IV– Um firewall NGFW funciona na forma mais simplificada que as demais categorias, filtrando apenas pacotes específicos.

Estão corretas:

A apenas II. B apenas II e III.

C apenas I, II e III. D apenas I, II e IV. E I, II, III e IV.

Questão 24

- (TRT 6, 2016)Entre as arquiteturas de Firewall, o Analista decidiu implantar a *Screened Host* no Tribunal Regional do Trabalho. Para isso, ele

A instalou dois roteadores em cascata para aumentar a segurança.

B isolou a rede interna utilizando uma DMZ.

C instalou um bastion host entre o roteador e a rede interna.

D criou três segmentos de redes, externa, interna e DMZ.

E instalou o roteador dentro da DMZ para maior proteção.

Questão 25

- Em relação à arquitetura de firewall, a preocupação reside na disposição dos equipamentos que compõem uma rede de computadores e o próprio firewall. Considere a separação entre a rede interna da organização da rede externa, que pode ser a internet, por meio da utilização de uma máquina que contenha duas interfaces de rede. Essa disposição consiste em uma arquitetura de firewall do tipo:

A Screened Host

B Dual-Homed Host

C Screened Subnet

D Screened-Homed

E Dual-Homed Subnet

Questão 26

- (AOCP, 2013 COREN-SC)Ao estabelecer-se uma VPN (Virtual Private Network) sobre a internet, em um projeto comum, são criados túneis entre as LANs que serão interligadas. Qual equipamento é utilizado para negociação de parâmetros, algoritmos e chaves entre as LANs?

A Placas de rede com WOL (Wake on LAN).

B Hub de conexão coaxial.

C Firewall.

D Patch panel.

E Cabo ótico com tecnologia de negociação.

Questão 27

- (INSTITUTO AOCP, 2019)Um firewall pode ser configurado com uma lista de regras baseadas em combinações com campos no cabeçalho IP ou TCP. Se houver uma correspondência com uma das regras, esta será usada para definir se encaminhará ou descartará o datagrama. Essa é uma característica de qual tipo de firewall?

A Intrusion Detection System.

B Proxy.

C Filtro de Pacotes.

D Statefull Inspection.

E Nível de aplicação.

Questão 28

- Considere que a arquitetura de firewall que examina os fluxos de tráfego de ponta a ponta na rede. Rápido, usa uma maneira inteligente de evitar o tráfego não autorizado, analisando os cabeçalhos dos pacotes e inspecionando o estado de cada um. É configurado para distinguir pacotes legítimos para diferentes tipos de conexões. Somente os pacotes que combinam a conexão ativa conhecida podem passar pelo firewall. É mais seguro que modelos básicos de filtragem de pacotes.

- Trata-se de

A packet widerange block.

B stateful packet inspection.

C screening router

D proxy service.

E screening filter.

Questão 29

- (VUNESP, 2019) O uso do recurso de NAT *(Network Address Translation*) na entrada de uma rede local, além de possibilitar a expansão da capacidade de endereçamento IP, apresenta a funcionalidade de um Firewall do tipo filtro de pacotes, pois

A IPs padrão de rede privada são utilizados para o envio dos pacotes para fora da LAN.

B pacotes nocivos gerados originalmente fora da LAN serão descartados quando recebidos pelo NAT.

C o NAT realiza a verificação do conteúdo dos pacotes da camada de Aplicação.

D o NAT cria uma região para a qual os pacotes com IPs privados são encaminhados e verificados antes de serem admitidos na LAN.

E o serviço transportado e identificado pela Porta TCP origem é criptografado quando do envio do pacote.

Questão 30

- (VUNESP, 2019) O protocolo que deve ser bloqueado no firewall para impedir que a máquina seja descoberta na rede pelo comando “ping” é o:

A DHCP

B GRE

C UDP

D ICMP

E TCP

Conclusão

- Conhecemos um pouco sobre Firewall e como se proteger.
- Não é a solução final para se proteger mas é começo.
- Ameaças surgem a cada instante portanto o estudo não para aqui.

Referências

- WEBER, Raul Fernando. Fundamentos de arquitetura de computadores. 4. ed. Porto Alegre: Bookman, 2012. E-book. Disponível em: https://integrada.minhabiblioteca.com.br/books/9788540701434

- STALLINGS, William. Arquitetura e organização de computadores. 8.ed. São Paulo: Pearson, 2010. E-book. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/459/epub/0

- HOGLUND, Greg. Como quebrar códigos: a arte de explorar (e proteger) software. São Paulo: Pearson, 2006. E-book. Disponível em: https://plataforma.bvirtual.com.br/Leitor/Publicacao/179934/epub/0

Fim