INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO RIO GRANDE DO NORTE

VITOR OLIVEIRA ROPKE

**TRABALHO SOBRE FIREWALL**

**SUMÁRIO**

[1 INTRODUÇÃO 2](#_Toc519497775)

[2 DESENVOLVIMENTO 3](#_Toc519497776)

[2.1 O QUE É UM FIREWALL 3](#_Toc519497777)

[2.2 COMO UM FIREWALL FUNCIONA 3](#_Toc519497778)

[2.3 QUAIS SÃO OS TIPOS DE FIREWALL QUE EXISTEM 3](#_Toc519497779)

[2.3.1 Packet filtering (filtragem de pacotes) 3](#_Toc519497780)

[2.3.1.1 Filtragem estática 3](#_Toc519497781)

[2.3.1.2 Filtragem dinâmica 3](#_Toc519497782)

[2.3.2 Proxy Services (proxy de serviços / firewall de aplicação) 4](#_Toc519497783)

[2.3.3 Stateful Inspection (inspeção de estados) 4](#_Toc519497784)

[2.4 COMO FUNCIONAM OS PROXIES SERVERS 4](#_Toc519497785)

[2.5 QUAIS SÃO AS ARQUITETURAS DOS FIREWALLS EXISTENTES 5](#_Toc519497786)

[2.5.1 Dual-Homed Host 5](#_Toc519497787)

[2.5.2 Screened Host 6](#_Toc519497788)

[2.5.3 Screened Subnet 6](#_Toc519497789)

[2.6 QUAIS SÃO OS PRINCIPAIS FIREWALL EXISTENTES NO MERCADO (COMERCIAL E LIVRE) 7](#_Toc519497790)

[3 CONCLUSÃO 8](#_Toc519497791)

[REFERÊNCIAS 9](#_Toc519497792)

# 1 INTRODUÇÃO

A internet é uma ferramenta utilizada por milhões de pessoas. É o lugar onde circula várias informações como senhas e dados bancários. Portanto é necessário ter alguma forma de proteger esses dados enquanto eles estão nas máquinas dos usuários ou circulando em redes internas.

O firewall é o sistema que irá proteger esses dados. Se configurado da forma correta ele pode impedir ataques de usuários mal-intencionados, entrada de malwares ou até impedir o acesso a sites.

No texto a seguir esclarecer-se-á as principais dúvidas sobre o firewall. Perguntas como “O que é um firewall”, “Como funciona um firewall”, “Quais os tipos de firewall” e outras são as mais comuns.

# 2 DESENVOLVIMENTO

## 2.1 O QUE É UM FIREWALL

Firewall é um sistema que serve para proteger uma rede. Como o próprio nome sugere (Fire – fogo e wall – muro) o firewall é uma barreira que executa ações determinadas nas regras configuradas. Pode bloquear ou permitir sites.

## 2.2 COMO UM FIREWALL FUNCIONA

O firewall funciona por meio de normas que, dependendo da ordem que foram colocadas, irão atuar sobre os pacotes entre a internet e a rede local. É necessário ter cuidado ao configurar regras pois, dependendo da regra, uma pode anular a outra. Após a configuração os dispositivos passam a estarem conectados ao firewall.

## 2.3 QUAIS SÃO OS TIPOS DE FIREWALL QUE EXISTEM

### 2.3.1 Packet filtering (filtragem de pacotes)

Aqui, o firewall faz a varredura do cabeçalho dos pacotes e faz as ações necessárias tal qual estão nas regras. Nesse tipo, o firewall faz regras sobre os protocolos, bloqueando ou liberando-os. O firewall de filtragem de pacotes possui dois tipos. Estático e dinâmico.

#### 2.3.1.1 Filtragem estática

O firewall executa as regras para todos os pacotes que estão ligados mesmo que a regra seja direcionada a um serviço específico. Isso gera problemas de segurança caso regras mais brandas sejam criadas para evitar bloqueio de pacotes importantes.

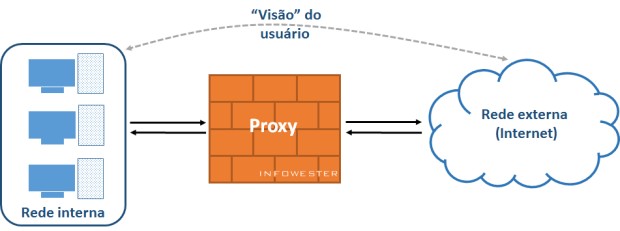
#### 2.3.1.2 Filtragem dinâmica

É uma adaptação da filtragem estática. As regras conseguem ser mais flexíveis, portanto, pacotes que fazem parte de um todo não sofrem bloqueios indevidos.

### 2.3.2 Proxy Services (proxy de serviços / firewall de aplicação)

Todos os pacotes passam pelo firewall e, então ele pode executar as regras necessárias para todos esses pacotes. Um proxy fica no meio do caminho entre a internet e o usuário. Ele pode controlar tudo o que o usuário acessa. Exemplo:

Imagem 1 - Proxy



Fonte: Site do INFOWESTER: O que é firewall? - Conceito, tipos e arquiteturas

### 2.3.3 Stateful Inspection (inspeção de estados)

É uma melhoria da filtragem dinâmica. Durante uma conexão os pacotes devem fluir por portas pré-definidas. Caso isso se altere, o firewall vai agir.

## 2.4 COMO FUNCIONAM OS PROXIES SERVERS

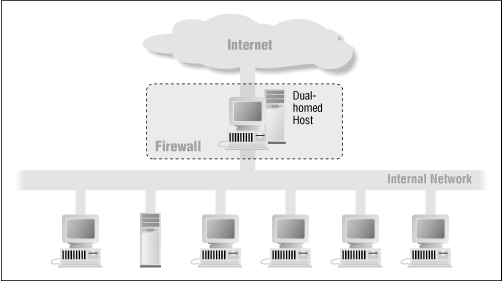
Ele faz as requisições de pacotes para a rede externa. Depois de se conectar ao endereço de destino ele passa os pacotes para a máquina que os solicitou. O IP que aparece no log do destino é o endereço do proxy, mantendo assim, o anonimato do IP da origem.

## 2.5 QUAIS SÃO AS ARQUITETURAS DOS FIREWALLS EXISTENTES

### 2.5.1 Dual-Homed Host

Funciona como um proxy. Todos os pacotes passam por um dispositivo chamado dual-homed host. Sua principal vulnerabilidade é a dependência desse computador para realizar a conexão. Em caso de ataques a rede pode parar, gerando prejuízos.

Imagem 2 - Dual-Homed Host

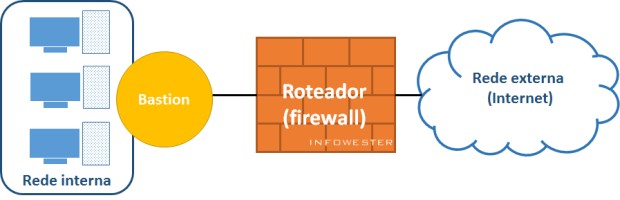


Fonte: Site do docstore

### 2.5.2 Screened Host

Parecido com a arquitetura Dual-Homed Host, porém possui um computador a mais chamado bastion host que fornece mais proteção à rede.

Imagem 3 - Arquitetura Screened Host

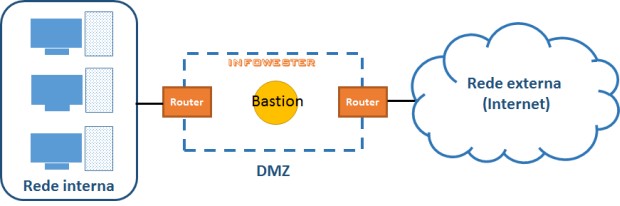


Fonte: Site do INFOWESTER: O que é firewall? - Conceito, tipos e arquiteturas

### 2.5.3 Screened Subnet

É a arquitetura mais segura. Possui uma zona desmilitarizada (DMZ) que é uma área isolada onde fica (m) o (s) bastion host (s) (pois pode ser implementado mais de um). DMZ fica entre a rede externa e interna. Essa arquitetura possui dois roteadores.

Imagem 4 - Arquitetura Screened Subnet



Fonte: Site do INFOWESTER: O que é firewall? - Conceito, tipos e arquiteturas

## 2.6 QUAIS SÃO OS PRINCIPAIS FIREWALL EXISTENTES NO MERCADO (COMERCIAL E LIVRE)

Comodo Firewall, ZoneAlarm, Jetico Personal Firewall, Filseclab Personal Firewall são os firewalls tanto comerciais como livres. O TinyWall é um firewall livre e o Norton 360 é comercial.

# 3 CONCLUSÃO

Esse trabalho esclareceu os principais questionamentos acerca do firewall. Vimos que um firewall possui três tipos que são Packet filtering (filtragem de pacotes), Proxy Services (proxy de serviços / firewall de aplicação) e Stateful Inspection (inspeção de estados). Possui também três arquiteturas. São elas Dual-Homed Host, Screened Host e Screened Subnet.

O firewall é mais comum para empresas, mas também é usado em redes domésticas. Existem então versões pagas que empregam maior segurança, mais opções de configuração, maior complexidade e versões gratuitas que possuem as funções fundamentais. Cabe à pessoa que irá utilizar o firewall saber a versão. Nem sempre o mais caro será o mais útil para quem irá utilizar o computador para tarefas básicas ou para pessoas comuns, da mesma forma que uma empresa grande não irá utilizar uma versão gratuita para protegê-la.

Portanto dá-se a importância do firewall para tornar redes mais seguras a medida que a internet cresce e mais pessoas passam a utilizá-la. Nesse crescimento progressivo as ameaças também seguem esse ritmo. É necessário ter cuidado ao acessar a internet. Seu correto uso pode coibir anormalidades na rede.

# REFERÊNCIAS

ALECRIM, Emerson. O que é firewall?: Conceito, tipos e arquiteturas. 2013. Disponível em: <https://www.infowester.com/firewall.php>. Acesso em: 14 jul. 2018.

BARWINSKIN, Luísa. O que é proxy?. 2008. Disponível em: <https://www.tecmundo.com.br/navegador/972-o-que-e-proxy-.htm>. Acesso em: 14 jul. 2018.

CHAPTER 4: Firewall Design. Disponível em: <https://docstore.mik.ua/orelly/networking/firewall/ch04\_02.htm>. Acesso em: 15 jul. 2018.

NOUIRA, Lucia. O que é um firewall? Como funciona?. 2012. Disponível em: <https://br.ccm.net/faq/12083-o-que-e-um-firewall-como-funciona>. Acesso em: 08 jul. 2018.

O QUE é um firewall?. Disponível em: <https://www.cisco.com/c/pt\_br/products/security/firewalls/what-is-a-firewall.html>. Acesso em: 08 jul. 2018.

O QUE é firewall?: Conceito, tipos e arquiteturas. 2017. Disponível em: <http://helpdigitalti.com.br/blog/o-que-e-firewall-conceito-tipos-e-arquiteturas/>. Acesso em: 14 jul. 2018.

PEREIRA, Ana Paula. Seleção: Firewalls. 2009. Disponível em: <https://www.tecmundo.com.br/seguranca/1374-selecao-firewalls.htm>. Acesso em: 14 jul. 2018.

QUAIS os tipos de firewall e suas diferenças?. 2015. Disponível em: <http://www.starti.com.br/blog/quais-os-tipos-de-firewal-e-suas-diferencas/>. Acesso em: 14 jul. 2018.