Cloud Computing

Gledson Scotti

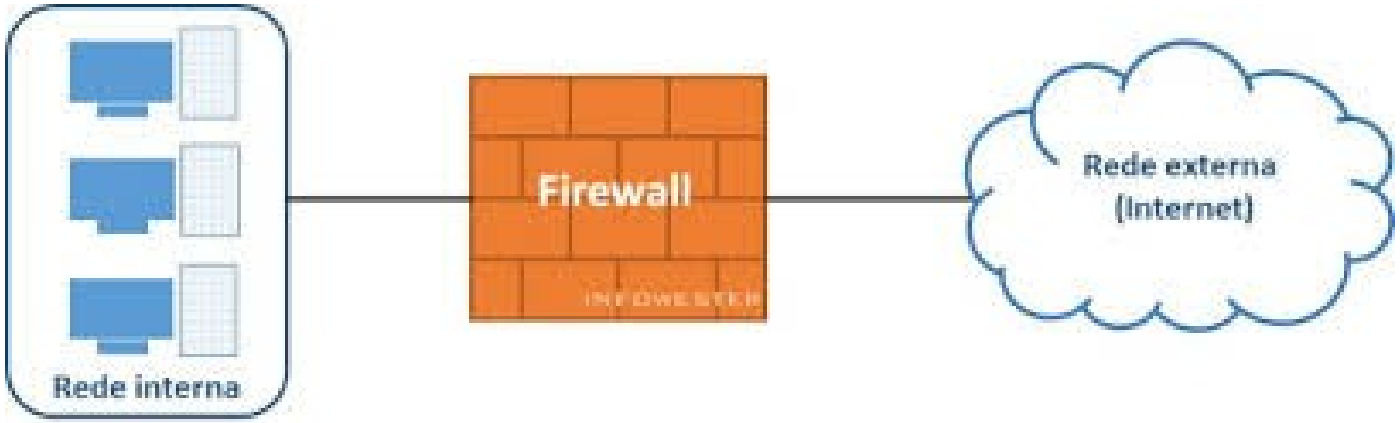
Firewall
Introdução

SATC
EDUCAÇÃO E TECNOLOGIA

Engenharia da Computação

O que é ...

Um firewall consiste em uma técnica de segurança de redes bastante efetiva. O seu nome vem das portas corta-fogo (firewalls) utilizadas em edifícios para conter o fogo de um possível incêndio, de modo que ele não se espalhe para o resto do prédio. Pode ser definido como um componente ou conjunto de componentes que restringem acesso entre uma rede protegida e a internet, ou entre outros conjuntos de redes.



Engenharia da Computação

O que é ...

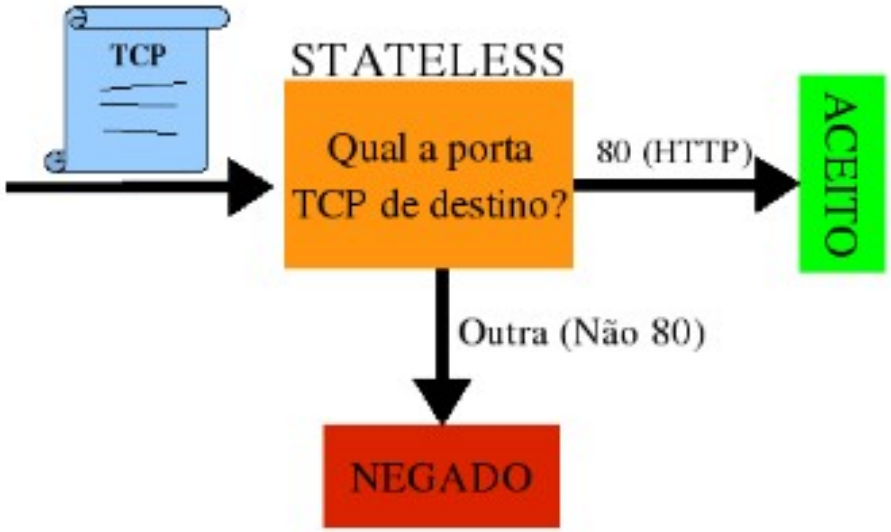
O firewall serve a múltiplos propósitos:

- Restringir a entrada de tráfego em um ponto único e controlado;
- Impedir que os atacantes consigam chegar em suas defesas mais internas;
- Restringir a saída de tráfego em um ponto único e controlado.

Deve ser visto como uma combinação de componentes (hardware, software e redes) objetivando proteger informações entre redes privada e a internet. Não pode ser visto como um “produto de prateleira”, para ser efetivo, necessita de planejamento e que seja definida uma topologia, onde ele esteja no meio das conexões que se deseja proteger.

Tipos de Firewall

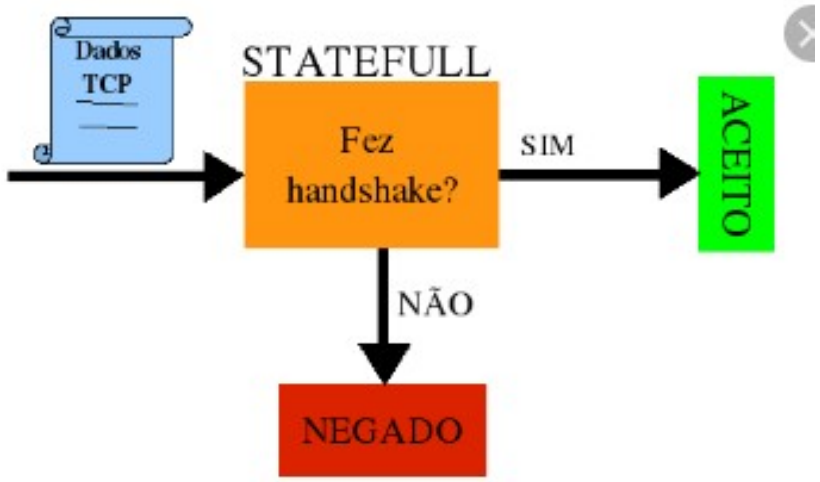
- Filtros de pacotes: Um filtro de pacote é capaz de decidir sobre a passagem ou não de um pacote, de acordo com as informações encontradas no cabeçalho IP;



***Stateless ou estático**: para aceitar o pacote basta o firewall analisar o conteúdo do atual pacote, olhando se a porta de destino dele é ou não porta 80. Se for, aceita, se não for, nega.*

Tipos de Firewall

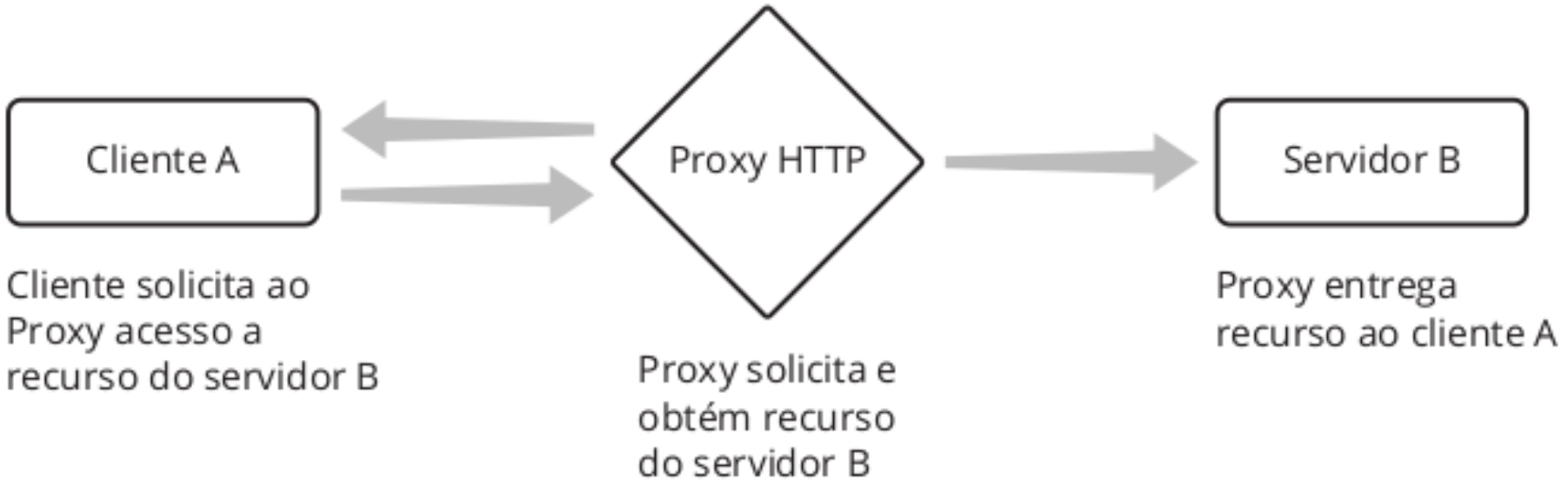
- Filtros de pacote dinâmicos: semelhante ao filtro de pacotes comum porém com maior inteligencia nas implementações das regras;



***Statefull ou dinâmico**: para aceitar o pacote é necessário que tenha ocorrido o handshake TCP. Se ocorreu, o firewall deve se lembrar, vendo em suas tabelas os pacotes anteriores. É chamado de dinâmico porque suas regras mudam de acordo com os pacotes que passam (fez handshake? Insere uma regra aceitando os dados)*

Tipos de Firewall

- Servidores proxy: Servidores proxy são servidores que acessam algum serviço da internet em nome de uma estação cliente;



Tipos de Firewall

- NAT: Network Address Translation (NAT) é um recurso que permite a modificação de um ende- RFC reço de rede em um pacote IP durante o seu trânsito em um dispositivo de roteamento.

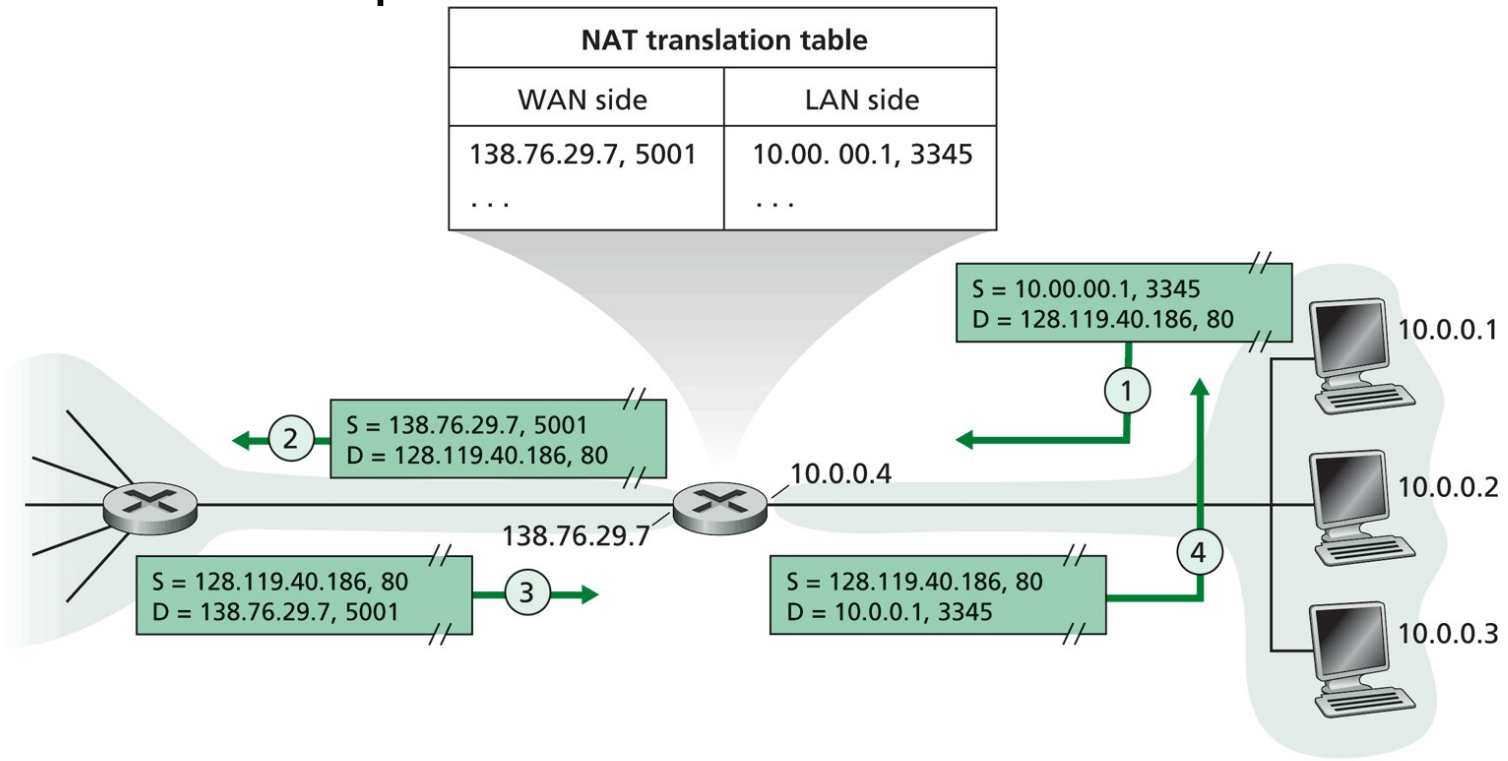


Figure 4.20 ♦ Network address translation

Engenharia da Computação

Tipos de Firewall

Existem tipos diferentes de NAT, com utilidades diferentes.

SNAT – Source NAT modifica o endereço IP de origem de um pacote, utilizado normalmente para permitir que estações em redes privativas possam acessar a internet diretamente, através da modificação do endereço privativo para um endereço válido na internet.

DNAT – Destination NAT modifica o endereço IP de destino de um pacote, utilizado normalmente para permitir que servidores em redes privativas possam ser acessados através da internet.

NAT estático – utiliza um endereço IP diferente para cada endereço que necessita ser traduzido. Também chamado de NAT um-para-um (1-1).

NAT dinâmico – traduz diversos endereços IP para um único endereço traduzido. Também chamado de NAT N-para-1 (N-1). Esse tipo de NAT permite que uma rede inteira acesse a internet utilizando um único endereço válido e muitas vezes é chamado de masquerading. Ele é usado por empresas que possuem poucos endereços IP validos.

Engenharia da Computação

Tipos de Firewall

UTM ou NGFW ? O Firewall de Próxima Geração ou Next-Generation Firewall (NGFW) e o Firewall de Gerenciamento Unificado de Ameaças ou Unified Threat Management (UTM) são projetados para fornecer um conjunto muito específico de serviços de segurança para as empresas.

O **firewall UTM** centraliza várias funções de segurança e produtividade, com mais facilidade de gestão e implantação. Mistura outras funções de segurança, como antivírus e proteção contra spam. Esses não são recursos de controle de acesso que normalmente definem um firewall, porém o mercado percebeu que os UTMs eram necessários não apenas para a funcionalidade de firewall, mas também para serviços de antimalware, antispam e filtragem de conteúdo. Tudo isso em um único sistema fácil de gerenciar.

O **Next Generation Firewall** é destinado a empresas com políticas de gerenciamento mais personalizadas. Um firewall faz o controle de acesso, basicamente decidindo quais aplicativos, portas, protocolos e usuários podem passar. O NGFW também pode procurar e negar o acesso, mas também com as ameaças. Os NGFW surgiram em resposta a empresas que queriam combinar a filtragem tradicional de portas e a capacidade de detectar tráfego na camada de aplicativos. Com o tempo, eles adicionaram mais recursos, como inspeção profunda de pacotes e detecção de malware.

Tipos de Firewall

Qual modelo de firewall escolher?

Modelos de **firewall UTM** fornecem políticas, gerenciamento e ferramentas de geração de relatórios prontos para uso. São projetados para facilitar a implantação e o gerenciamento contínuo.

Já os **NGFW** atendem organizações que desejam personalizar suas políticas de segurança e preferem técnicas manuais de relatório e gerenciamento.

Em um ponto de vista geral, os dispositivos fazem praticamente a mesma coisa, porém cada empresa precisa se concentrar no que é importante: o dispositivo deverá ser dimensionado para atender os volumes de tráfego e todos os serviços utilizados !

Exemplo: https://www.symmetry.com.br/next-generation-utm-firewall/

Tipos de Firewall

Marcas conhecidas de Firewall

SONICWALL

NETDEEP SECURE 3.4

NEXT GENERATION OPEN SOURCE FIREWALL

paloalto NETWORKS

pfsense

FORTINET

SOPHOS

OPNsense® **FEATURES**

Free & Open source - Everything essential to protect your network and more