atec

Firewall

Formador: Pedro Sardinha

Segurança em Sistemas Informáticos

Objetivos especificos

- Tipologia
- Filtros de pacotes
- Filtro de circuito
- Ponte aplicacional

Segurança em Sistemas Informáticos

Objetivos especificos

- Tipologia
- Filtros de pacotes
- Filtro de circuito
- Ponte aplicacional

Segurança em Sistemas Informáticos

Introdução

- Na internet e redes de computadores – Perigos!
- Por esta razão que é importante conhecer e utilizar ferramentas de proteção para computadores e redes.
- Firewall – uma das opções de segurança mais importante na informática

Segurança em Sistemas Informáticos

O que é uma firewall?

- Solução de segurança baseada em hardware ou software.
  - Conjunto de regras ou instruções
  - Analisa o tráfego de rede – determina quais as operações de transmissão ou recepção de dados podem ser executadas.

  - Barreira de defesa
    - Bloqueia o tráfego de dados indesejado e permite acessos desejados.

Segurança em Sistemas Informáticos

O que é uma firewall?

- Como uma portaria:
  - Para entrar é necessário obedecer a determinadas condições:
    - Como se identifica?
    - Quem o espera?
    - Traz algum objecto que possa trazer riscos de segurança?
    - Ao sair – não pode levar nada sem devida autorização.
  - Impede uma série de atos maliciosos
    - Exemplo – malware
    - Usa um porto para se instalar num computador sem o utilizador saber.
    - Programa que envia dados sigilosos para a internet
    - Tentativa de acesso à rede a partir de computadores externos não autorizados
    - Entre outros

Segurança em Sistemas Informáticos

Como funciona?

- Espécie de barreira que verifica quais dados podem passar ou não.
  - Só é possível mediante o estabelecimento de políticas – regras.

- Pode ser configurado para bloquear todo e qualquer tráfego no computador ou na rede.
  - Isola um computador ou rede.

Como funciona?

- Permitir automaticamento o tráfego de determinados tipos de dados
  - Pedidos HTTP (páginas Web)

- Bloquear outras
  - Ligações de serviço de email.

Como funciona?

- As politicas de firewall são baseadas inicialmente em dois princípios:

    1. Todo tráfego é bloqueado, excepto o que está explicitamente autorizado.

    2. Todo tráfego é permitido, excepto o que está explicitamente bloqueado.

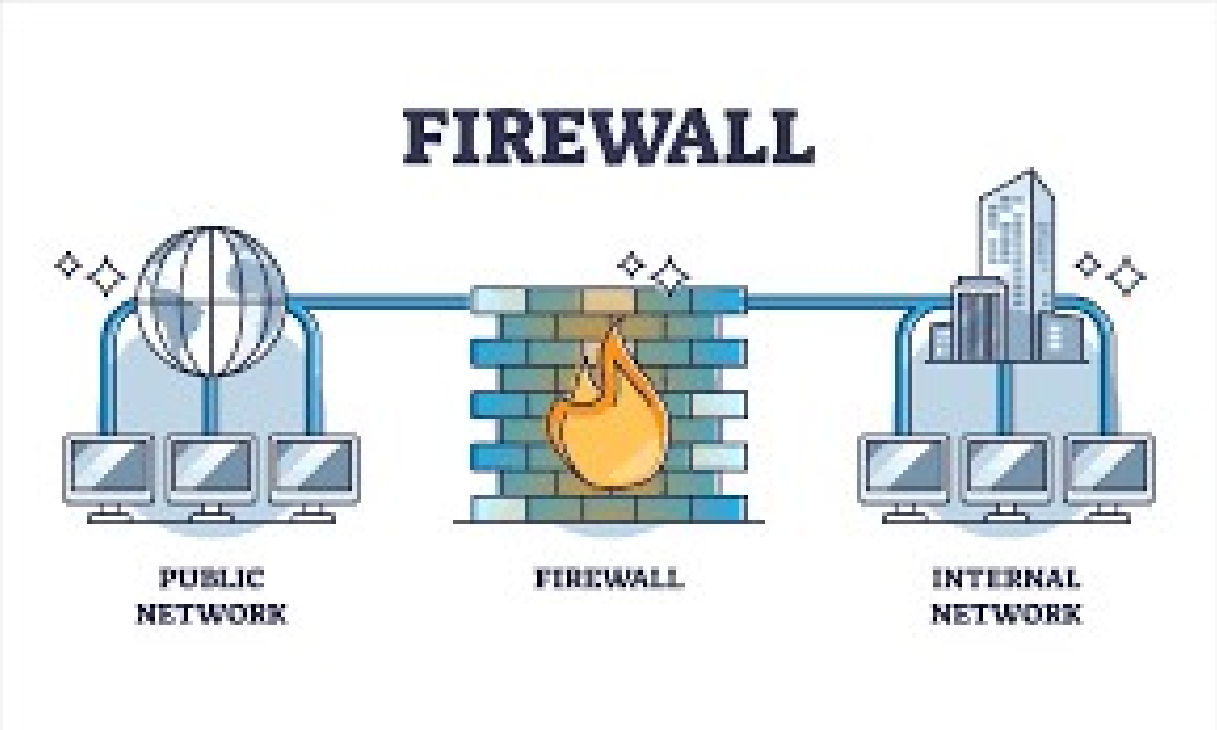
Segurança em Sistemas Informáticos

Como funciona?

- Firewalls mais avançadas
  - Direcionar o tráfego para sistemas de segurança internos mais específicos
  - Oferecem reforço extra em procedimentos de autenticação de utilizadores
  - Entre outros

Segurança em Sistemas Informáticos

Firewall



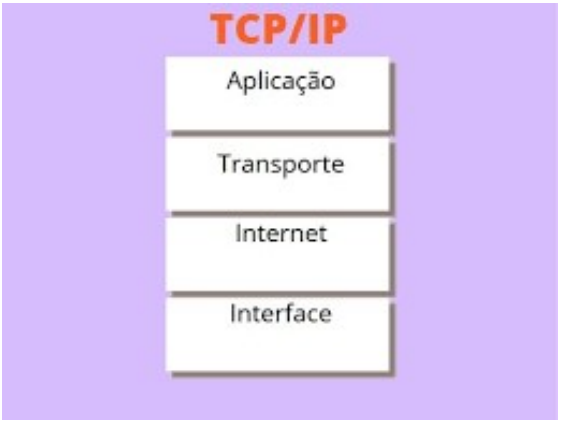
Tipos de Firewall

- Filtros de pacotes (packet filtering)
  - Primeiras soluções de 1980
  - Baseado em filtros de pacotes de dados (packet filtering)
  - Mais simples e limitada – nível de segurança significativo

  - Saber o que cada pacote possui um cabeçalho com diversas informações:
    - Endereço IP Origem e Destino
    - Tipo de Serviço
    - Tamanho
    - Entre outros

Segurança em Sistemas Informáticos

Tipos de Firewall



- Filtros de pacotes (packet filtering)
  - Transmissão de dados – TCP/IP
    - Feito por camadas
- A filtragem limita-se às camadas de rede e transporte
  - **Rede** – onde ocorre o endereçamento dos equipamentos que fazem parte da rede e roteamento
  - **Transporte** – onde estão os protocolos que permitem o tráfego de dados (TCP e UDP)

Exemplo – uma regra que permite todo o tráfego da rede local que utiliza a porta UDP 123; ou uma politica que bloqueia qualquer acesso da rede local por meio da porta TCP 25 (SMTP).

Segurança em Sistemas Informáticos

https://www.youtube.com/watch?v=6GXZ8_TiW

Tipos de Firewall

- Filtros de pacotes (packet filtering)
  - Filtragem estática
    - Bloqueia ou permite os dados com base em regras
      - Não importa a ligação que um pacote tem com outro.
    - Pode ser um problema – porque determinados serviços ou aplicações podem depender de respostas ou pedidos específicos para iniciar e manter a transmissão
      - Filtro pode permitir o tráfego dos serviços – mas bloqueia respostas/pedidos necessários para executar a tarefa.
      - Limita na criação de regras mais abrangentes e menos rígidas – pode provocar tráfego indesejado.
  - Filtragem dinâmica
    - Surge para superar as limitações dos filtros estáticos
    - Consideram o contexto em que os pacotes estão inseridos para criar regras que se adaptam a esse cenário – permite o fluxo das respostas.

Segurança em Sistemas Informáticos

Tipos de Firewall

https://www.youtube.com/watch?v=uPnQL2AcPeM

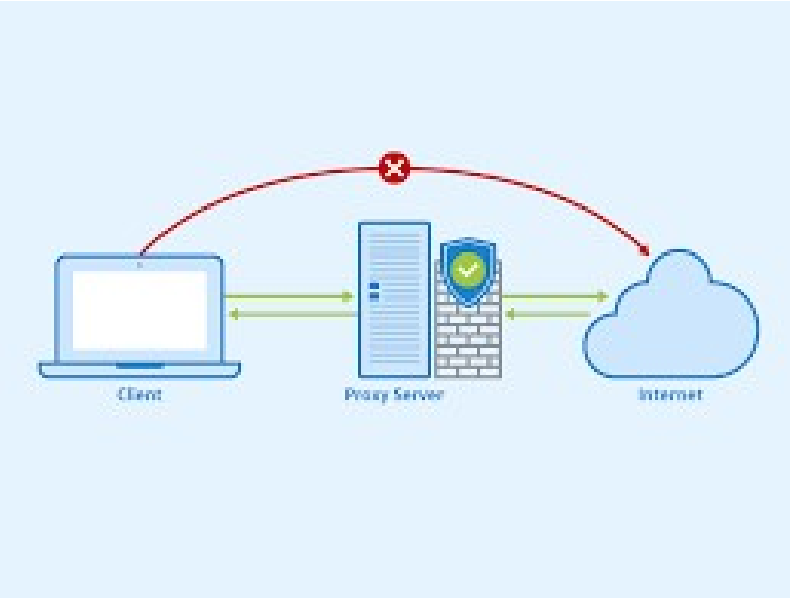
- Filtros de circuito
  - Consome menos recursos de computação
  - Verifica o handshake do protocolo de comunicação (TCP)
    - Sessão de pacote legitima.

  - Eficientes em recursos mas não verificam o pacote (analisam)
    - Se o pacote tiver malware mas tem o handshake correto, o tráfego é permitido
    - Não são suficientes para proteger a rede.

Segurança em Sistemas Informáticos

Tipos de Firewall

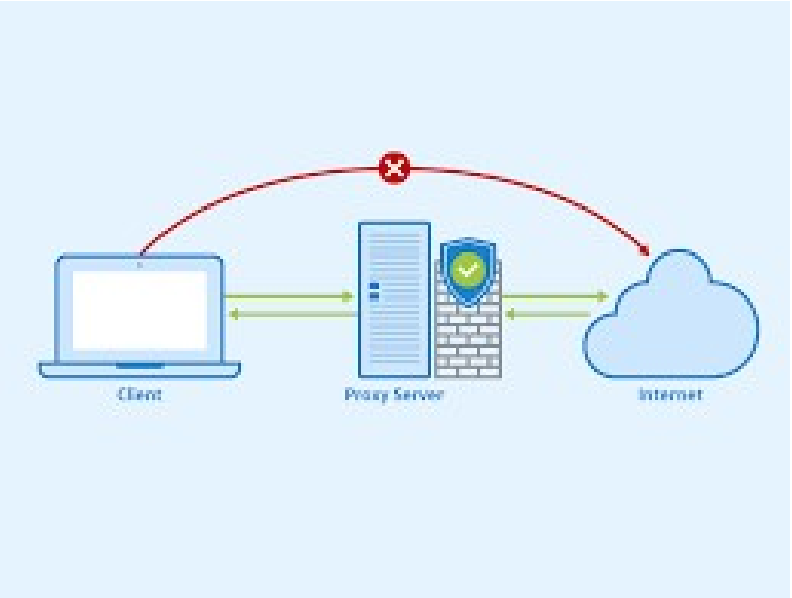
- Firewall de aplicação ou proxy
  - Atua como intermediário entre um computador ou uma rede interna e outra rede (externa)
    - Exemplo – Internet
    - Servidores potentes – lidam com grande número de solicitações
    - Solução interessante – não permite a comunicação direta entre origem e destino



Segurança em Sistemas Informáticos

Tipos de Firewall

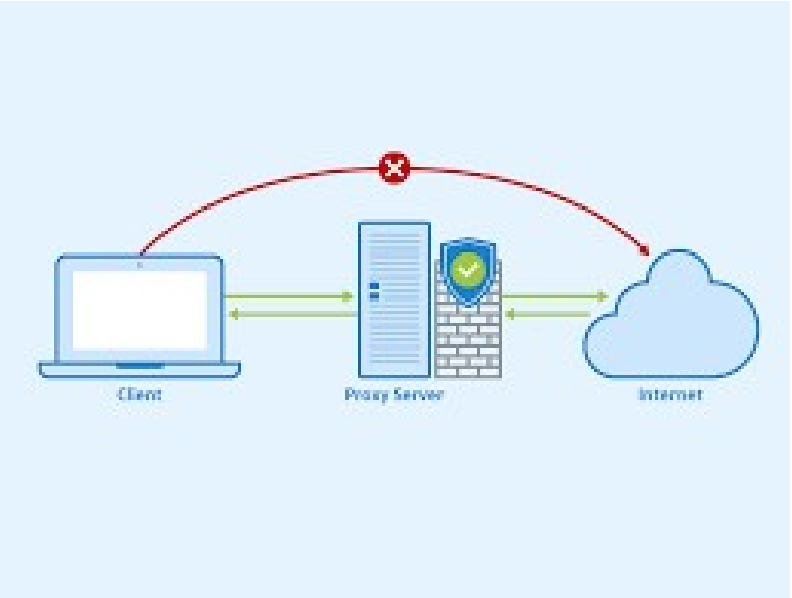
- Firewall de aplicação ou proxy
  - Possível estabelecer regras que impeçam o acesso de determinados endereços externos
  - proíbam a comunicação entre computadores internos e determinados serviços remotos.



Segurança em Sistemas Informáticos

Tipos de Firewall

- Firewall de aplicação ou proxy
  - Possível estabelecer regras que impeçam o acesso de determinados endereços externos
  - proíbam a comunicação entre computadores internos e determinados serviços remotos.

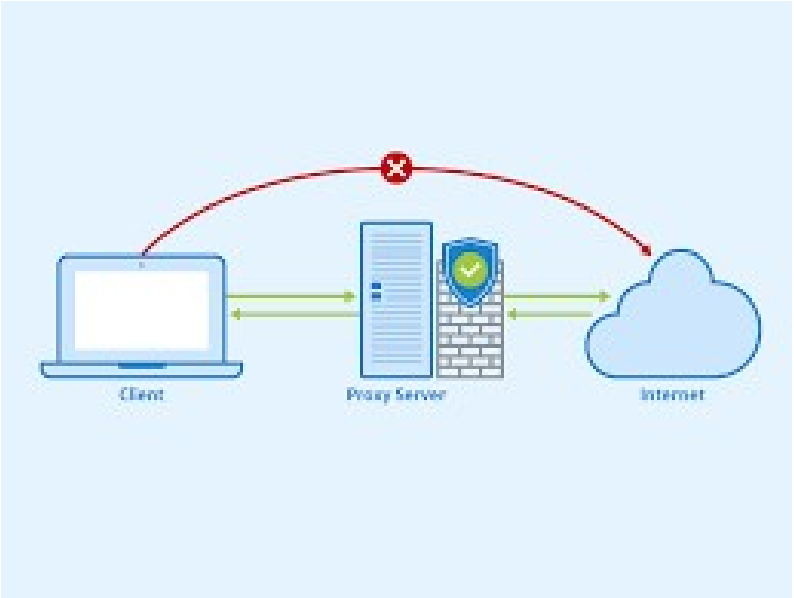


Segurança em Sistemas Informáticos

Tipos de Firewall

https://www.youtube.com/watch?v=RxGfkt3Vy8

- Firewall de aplicação ou proxy
  - Tarefas complementares:
  - o equipamento pode registrar o tráfego de dados em um arquivo de log
  - Espécie de cache – Página Web, faz com que fique guardada e não seja necessário fazer sempre o pedido ao endereço original



Segurança em Sistemas Informáticos

Tipos de Firewall - Firewall de aplicação ou proxy

- Proxy transparente
  - 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.
    - Torna o trabalho de configuração inviável e moroso.
  - Surge como alternativa – as máquinas da rede não precisam de saber da sua existência
    - Dispensa qualquer configuração específica.
  - Todo o acesso é feito – cliente para rede externa e vice-versa.
    - O proxy transparente consegue intercepta-lo e responder como se fosse uma comunicação direta.

Tipos de Firewall - Firewall de aplicação ou proxy

- Proxy transparente – Desvantagens
  - um proxy "normal" é capaz de barrar uma atividade maliciosa
    - malware envia dados de uma máquina para a internet
  - proxy transparente, por sua vez, pode não bloquear este tráfego

Tipos de Firewall

- Inspeção de estados (stateful inspection)
  - Evolução dos filtros dinâmicos
  - Fazem comparação entre o que está a acontecer e o que é esperado acontecer.
  - Analisam todo o tráfego de dados para encontrar estados (padrão)
    - Padrões aceitáveis por regras
    - Usados para manter a comunicação

https://www.youtube.com/watch?v=3UMU2cyq

Tipos de Firewall

- Inspeção de estados (stateful inspection) - Exemplo
  - Aplicação inicia uma transferência de dado entre cliente e servidor
  - Pacotes iniciais informam – portas TCP usadas

  - Se o tráfego começa a fluir por outra porta não mencionada
    - Firewall deteta a anomalia e faz o bloqueio.

PALMELA
Edifício ATEC · Parque Industrial da Volkswagen Autoeuropa
2950-557 · Quinta do Anjo
Tel. 212 107 300 | info@atec.pt

PORTO
Edifício Siemens · Av. Mário Brito (EN107), nº 3570 · Freixieiro
4456-901· Perafita
Tel. 220 400 500 | infoporto@atec.pt

www.atec.pt