UFU - Universidade Federal de Uberlândia

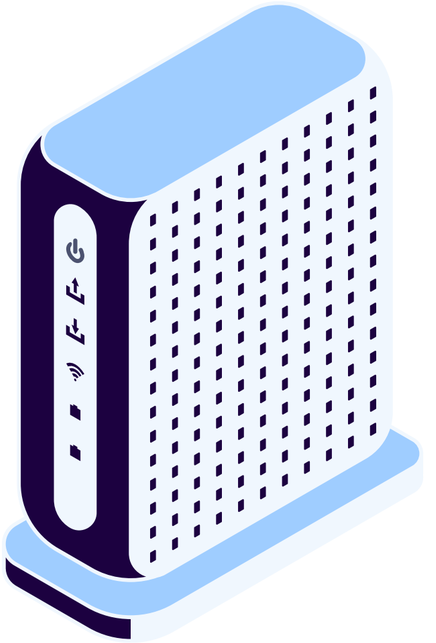
Redes de Computadores

FIREWALLS

Alunos: Ana Clara, Áthina e Lucas Flores

SEGURANÇA CRÍTICA

A dependência das empresas em relação à internet cresceu exponencialmente. Hoje, a conectividade é vital não apenas para a comunicação, mas também para operações diárias, gestão de dados e relacionamento com clientes. Garantir a segurança dos ativos de rede deixou de ser uma questão técnica e se tornou uma preocupação fundamental de negócios.



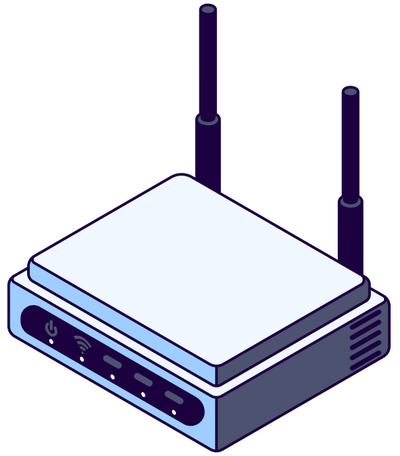
A necessidade de segurança em redes é mais urgente do que nunca. Para resolver esse problema: O firewall

O FIREWALL COMO SOLUÇÃO!!!!!

Firewalls são tipicamente usados em segurança de redes para proteger uma rede confiável (como a sua casa ou escritório) de uma rede não confiável (como a internet).

Essa proteção é oferecida pelo firewall ao monitorar o tráfego de rede que entra e sai. Se o tráfego for considerado suspeito, ele é geralmente bloqueado e o usuário é notificado

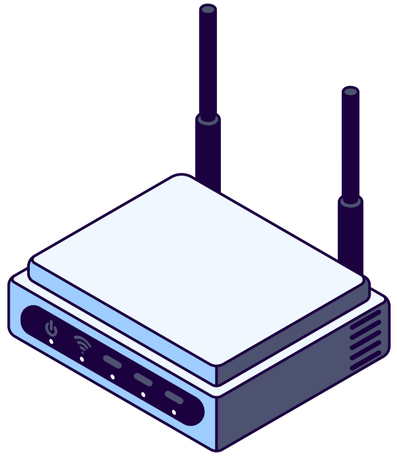
Firewalls de hardware são integrados em dispositivos de rede, como roteadores. Já os firewalls de software são instalados em um sistema operacional. É comum que uma rede tenha múltiplos firewalls para protegê-la.



OBJETIVOS FIREWALL

Os firewalls possuem três objetivos fundamentais:

- Controle Total do Tráfego
- Segurança.
- Resistência à Penetração



filtro de pacotes tradicionais

Os filtros de pacotes tradicionais operam na camada de rede, inspecionando cada pacote de dados individualmente em roteadores de borda.

Critérios de Filtragem

- **Endereços:** IP de origem e destino.
- **Protocolos:** TCP, UDP, ICMP, OSPF.
- **Portas:** TCP ou UDP de origem e destino.
- **Flags TCP:** SYN, ACK.
- **Regras:** Diferentes para tráfego de entrada e saída, e para diferentes interfaces.

Limitações

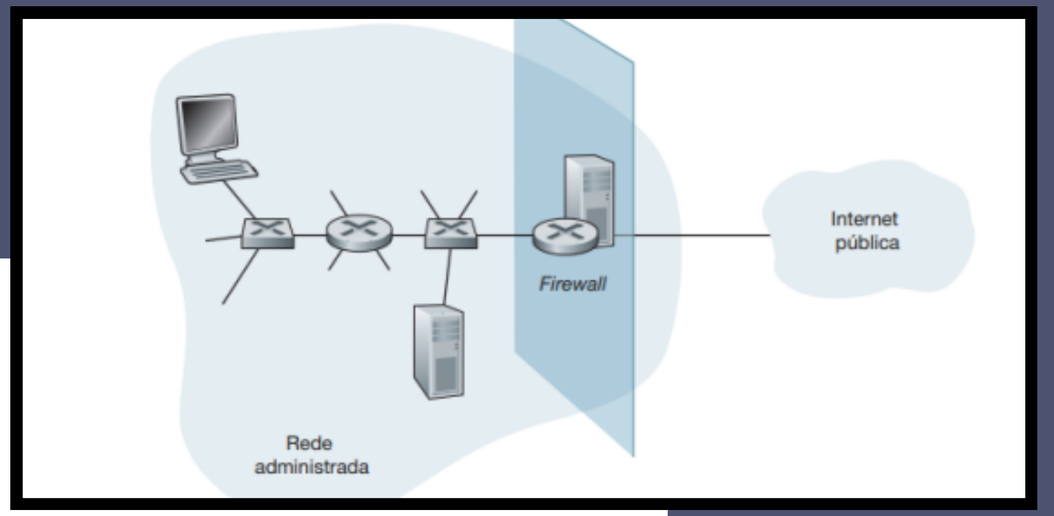
- **Análise individual:** Não conseguem entender o contexto de uma conexão.
- **IP Spoofing:** Não protegem contra pacotes com endereços de remetente falsos.
- **Ataques complexos:** Dificuldade em identificar ataques que usam sequências de pacotes.

LISTAS DE CONTROLE DE ACESSO (ACLS)

As ACLs (Listas de Controle de Acesso) são a forma mais comum de aplicar as regras dos filtros de pacotes tradicionais.
São conjuntos de regras ordenadas que agem como a "linguagem" de programação do firewall.

Elas instruem roteadores e switches a permitir ou negar o tráfego com base em critérios como endereços IP e portas.

FILTROS DE ESTADO (STATEFUL FILTERS)



DIFERENCIAL

- Não analisam cada pacote individualmente.
- Consideram o contexto de toda a conexão.
- Isso permite uma proteção mais inteligente e a capacidade de diferenciar tráfego legítimo de ataques.

VANTAGEM:

- Correção de falhas: Corrigem a principal limitação dos filtros de pacotes tradicionais, que não conseguem identificar o estado da conexão.
- Resistência a ataques: Bloqueiam pacotes maliciosos, como aqueles com flags TCP manipuladas
- Segurança aprimorada: Proporcionam uma camada de segurança mais robusta, pois validam a legitimidade da comunicação desde o início.

FILTROS DE ESTADO (STATEFUL FILTERS)

COMO FUNCIONA:

O firewall registra na tabela dados como endereços IP e portas de cada comunicação, do início ao fim.

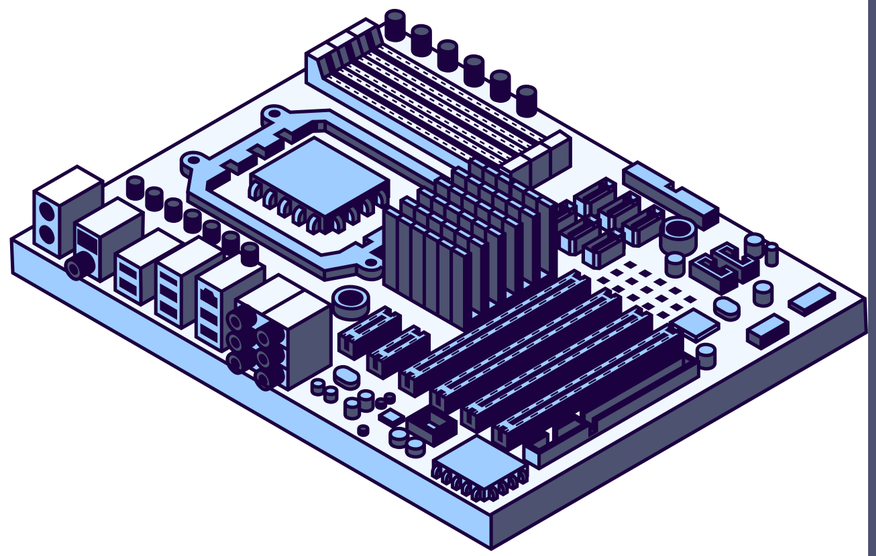
- O firewall monitora a troca inicial de mensagens (SYN, SYN/ACK, ACK) para validar uma conexão legítima.
- Quando um pacote de resposta (com a flag ACK) chega, o firewall consulta sua tabela de estado.
- Se a conexão estiver registrada e validada, o pacote é liberado.
- Se o pacote não corresponder a nenhuma conexão na tabela, ele é automaticamente bloqueado, mesmo que os IPs e portas pareçam corretos.

Ação	Endereço de origem	Endereço de destino	Protocolo	Porta de origem	Porta de destino	Bit de flag
Permitir	222.22/16	Fora de 222.22/16	TCP	> 1023	80	Qualquer um
Permitir	Fora de 222.22/16	222.22/16	TCP	80	> 1023	ACK
Permitir	222.22/16	Fora de 222.22/16	UDP	> 1023	53	—
Permitir	Fora de 222.22/16	222.22/16	UDP	53	> 1023	—
Negar	Todos	Todos	Todos	Todos	Todos	Todos

GETAWAY DE APLICAÇÃO

Os Gateways de Aplicação operam na camada de aplicação, inspecionando o conteúdo do tráfego para uma segurança mais precisa.

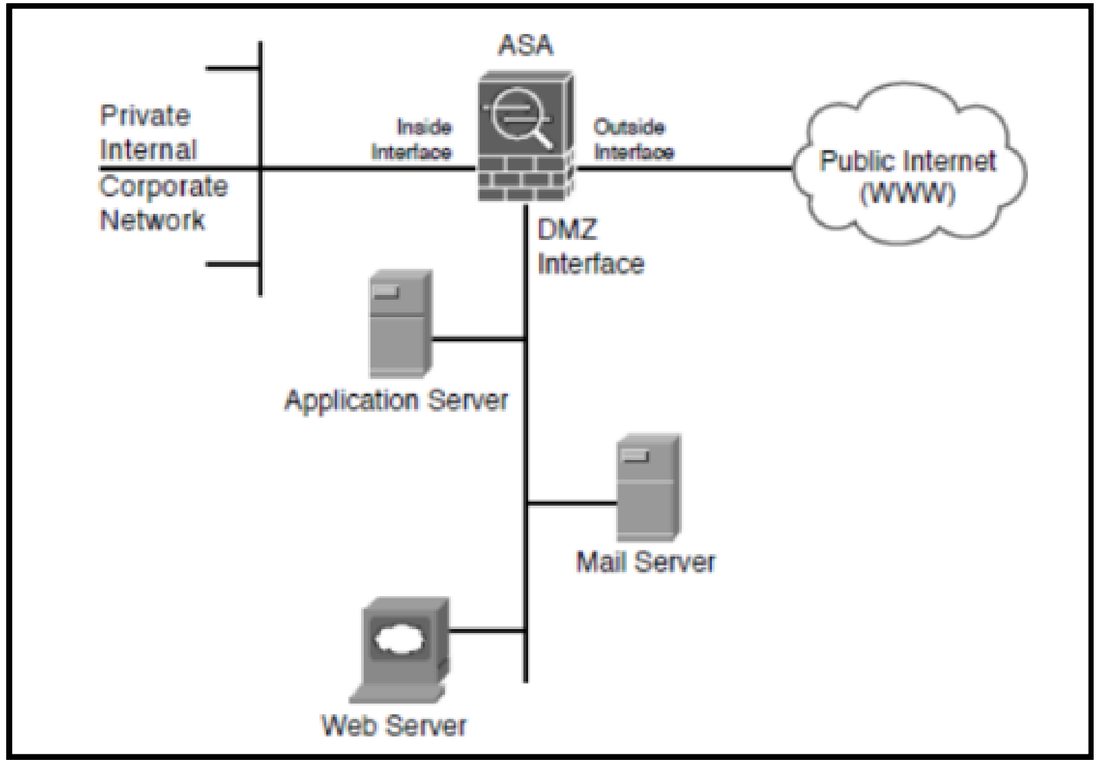
- **Funcionamento como Intermediários:** Eles agem como servidores proxies, administrando o fluxo de dados entre as redes.
- **Inspeção Detalhada:** A sua principal vantagem é a capacidade de analisar além dos cabeçalhos de rede, examinando o conteúdo da aplicação.
- **Uso Específico:** Cada gateway é um servidor distinto, dedicado a uma aplicação específica (ex: um para tráfego HTTP, outro para FTP, etc.), garantindo um controle mais rigoroso.



ZONA DESMILITARIZADA (DMZ)

sub-rede intermediária que atua como uma zona neutra entre sua rede interna privada e a internet

- Isola e proteger a infraestrutura principal da sua organização.
- Permite que serviços públicos, como servidores web, FTP e e-mail, operem em um ambiente separado e controlado.
- Garante que o acesso da internet seja limitado apenas aos servidores na DMZ, impedindo que ele chegue diretamente à sua rede interna. Essa barreira é aplicada e fiscalizada por políticas de segurança no firewall.

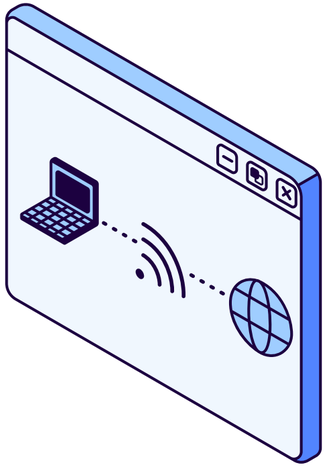


ARQUITETURA DMZ

DMZ: Opções de Arquitetura

- Firewall Único:

Este modelo utiliza apenas um firewall para criar a DMZ, que o conecta à internet, à rede interna e à própria zona desmilitarizada. Embora seja a abordagem mais simples e econômica, ela é considerada a mais vulnerável. Como é um ponto único de falha, se o firewall for comprometido, toda a rede fica exposta.



- Múltiplos Firewall:

Este modelo usa dois ou mais firewalls para criar camadas de proteção, sendo um entre a internet e a DMZ, e outro entre a DMZ e a rede interna. Apesar de ser mais complexa e custosa, oferece uma segurança muito superior. Para um atacante, é significativamente mais difícil invadir a rede, já que ele precisaria ultrapassar as barreiras de mais de um firewall.

Firewalls

Desvantagens

- **Falsa sensação de segurança** - Firewall mal projetado pode ser pior que nenhum.
- Impacto no **desempenho da rede** - tráfego passa por um único ponto
- **Complexidade** de implementação e gestão - Não é “plug and play”.
- Requer **configuração** detalhada e **manutenção** constante.
- **Risco de bloquear serviços** legítimos e prejudicar a produtividade.

Limitações

Limitações dos métodos de filtragem

- Filtros de pacotes:
  - Analisam pacotes isolados (sem contexto).
  - Não inspecionam conteúdo real.

- Evolução para firewalls stateful e gateways para superar limitações.

tipos de Firewall

Filtros de Pacotes Tradicionais

- Simples de implementar (ex.: iptables).
- Flexibilidade de regras e interfaces.
- Configuração por políticas da organização.

Filtros de Pacotes com Estado (Stateful)

- Mantém tabela de conexões ativas.
- Maior segurança contra ataques sofisticados.
- Detecta início/fim de conexões (SYN, ACK, FIN).
- Prevenção contra pacotes defeituosos.

Getaways

Vantagens

- Inspeção profunda (camada de aplicação).
- Autenticação de usuários.
- Funcionalidade de proxy.
- Suporte a múltiplas aplicações (HTTP, FTP, e-mail etc.).
- Controle baseado em identidade e credenciais.

Limitações

- Necessidade de um gateway para cada aplicação.
- Impacto no desempenho (risco de gargalo).
- Configuração complexa (cliente precisa conhecer o gateway).

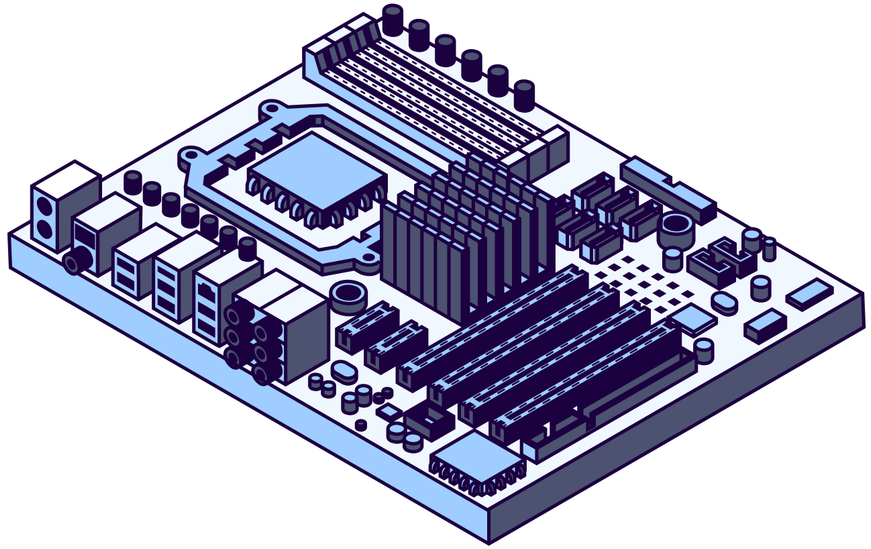
APLICAÇÃO

Dividida em 3 partes:

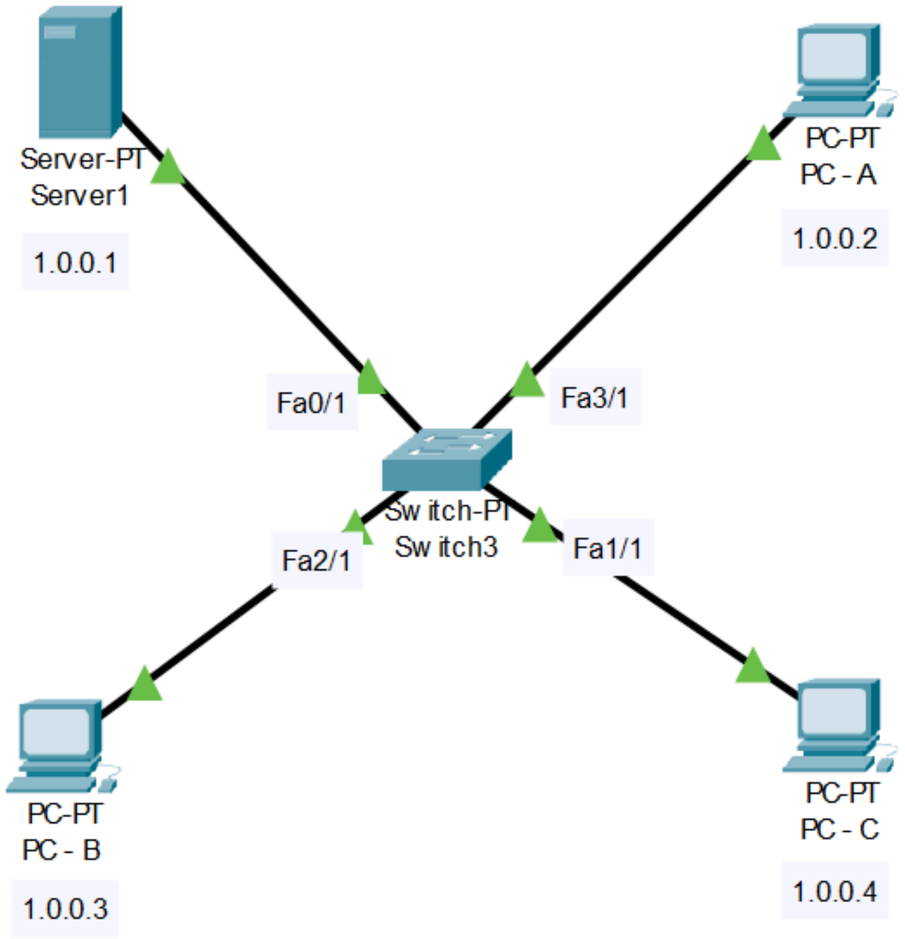
1º Fase: Topologia Básica

2º Fase: Topologia Avançada

3º Fase: Implementação Física



1º FASE



TOPOLOGIA

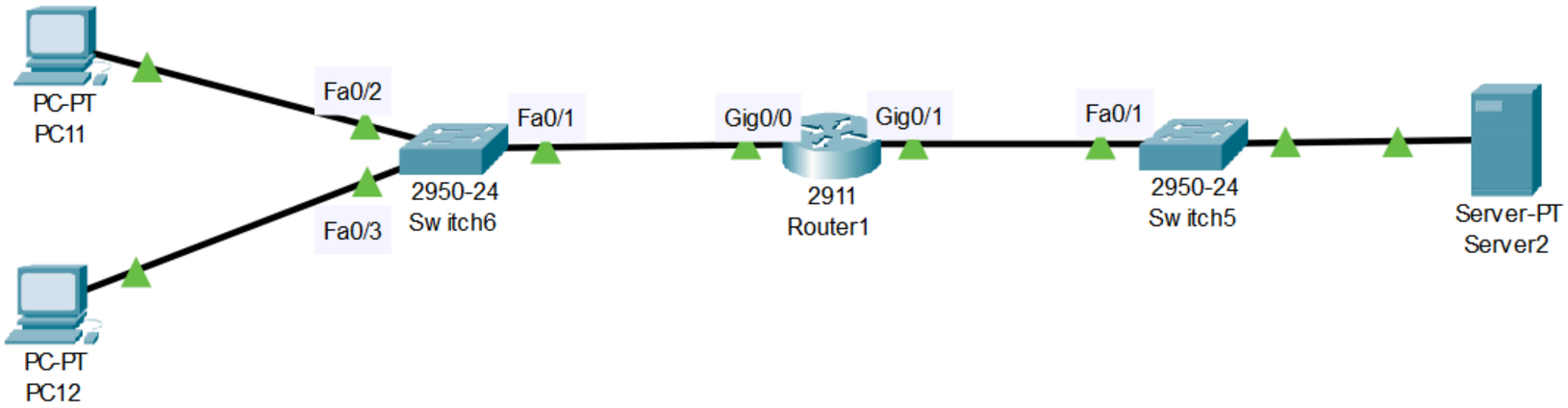
- 3PCs + 1 Servidor

IMPLEMENTAÇÃO

- Firewall no servidor bloqueando ICMP e permitindo IP

RESULTADOS

- Ping bloqueado
- Acesso web permitido



2° FASE

TOPOLOGIA

- LAN interna + DMZ
- Roteador com ACLs estendidas

APLICAÇÃO

- Permitir gerenciamento do roteador pela LAN
- Permitir HTTP da LAN para a DMZ
- Negar todo o resto

RESULTADOS

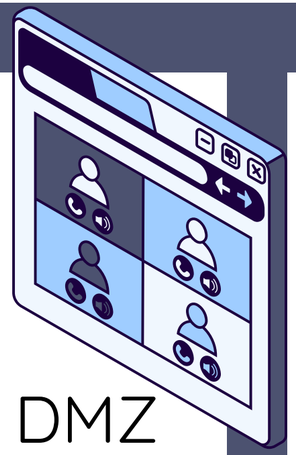
A validação das configurações foi feita a partir de uma série de testes:

Teste 1

Ping para o roteador

ping 10.0.0.1

✅ Permitido

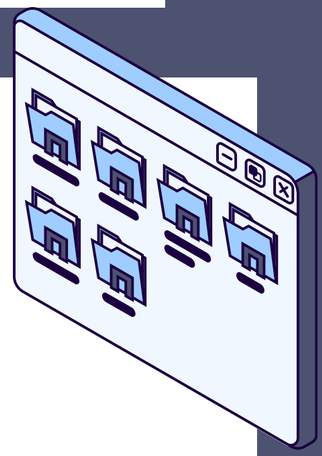


Teste 2

Acesso HTTP ao servidor na DMZ

http://192.168.1.10

✅ Permitido



Teste 3

Ping para o servidor

ping 192.168.1.10

🚫 Negado

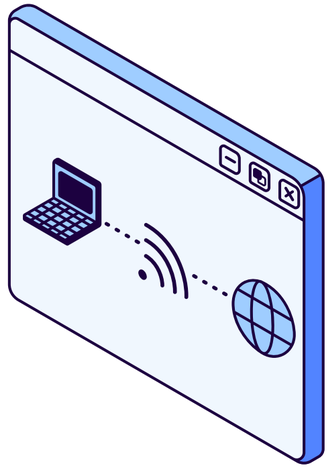
3º FASE

AMBIENTE

- Linux MiniOS rodando via pendrive
- Uso do iptables para filtragem
- Bloqueio de URL específica (Facebook)

COMANDOS USADOS:

- nslookup para obter IP
- iptables para bloquear faixas de IPs



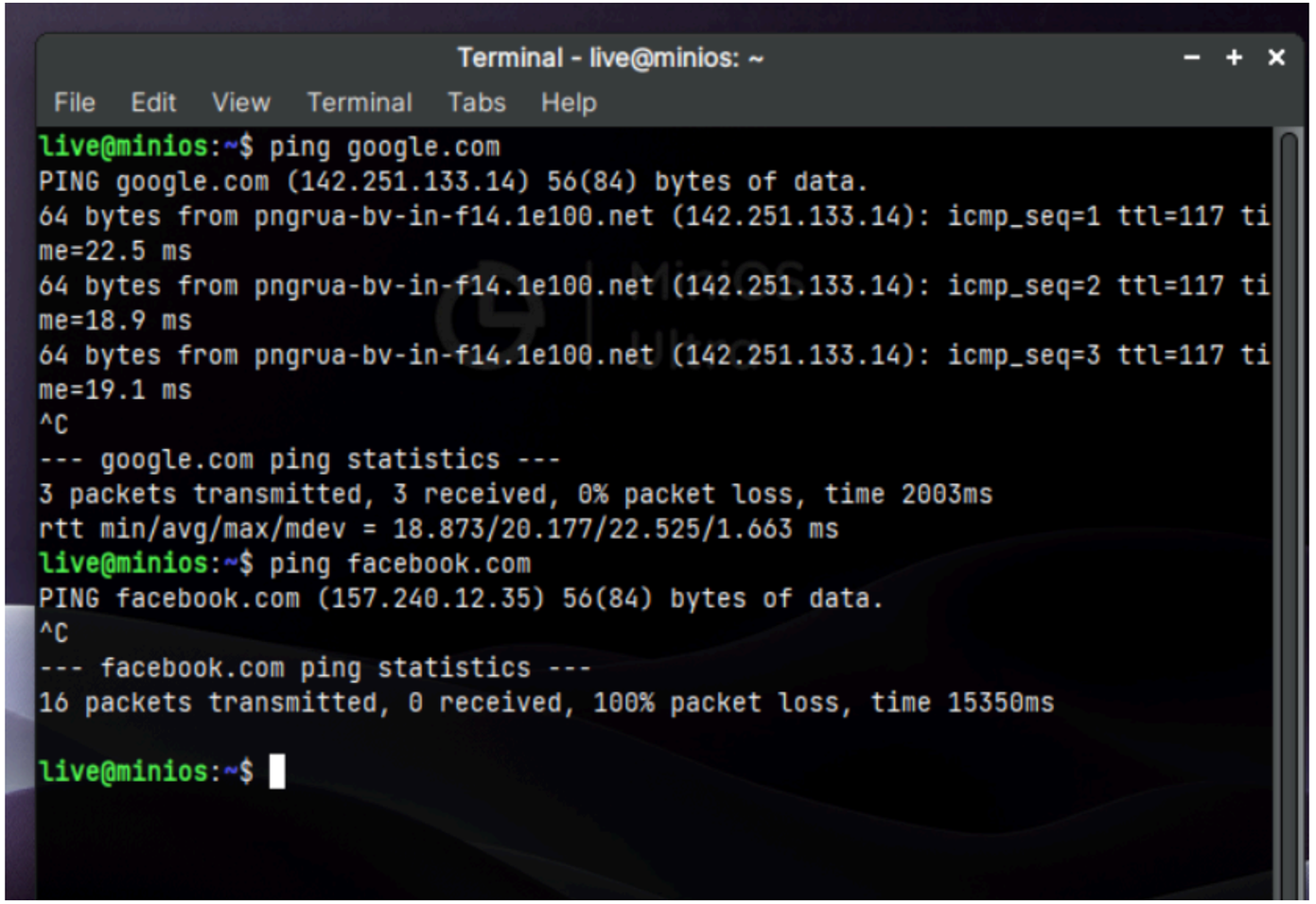
RESULTADOS

Testes Realizados

- ✅ Ping para o Google
- 🚫 Ping para o Facebook

Navegação

- ✅ Google e YouTube
- 🚫 Facebook e WhatsApp



CONCLUSÃO

Firewalls são eficazes, mas dependem de configuração

DMZ e segmentação aumentam a segurança

ACLs e iptables permitem controle granular