



UNIVERSIDADE
FEDERAL DO CEARÁ
Campus de Quixadá

Informações importantes:

- **Segunda Avaliação Parcial**
- equipe: **3 alunos**
- Datas importantes
 - entrega: dia **05//07/23** via **SIGAA**.
 - **Documentação** (parte lógica: topologia + configurações)
 - Apresentação: 05 e 07/07/23
 - **VMs em execução com demonstração dos acessos**

Descrição Geral:

O aluno deve aplicar os conhecimentos adquiridos sobre firewall e proxy em um cenário de rede real para proteger a rede interna de acessos externos, ao mesmo tempo, que permite o acesso ao servidor WEB da organização.

A figura 1 abaixo ilustra o cenário de rede de uma organização em que o *netfilter* controla os acessos internos e externos e squid gerencia o tráfego WEB da rede interna cliente.

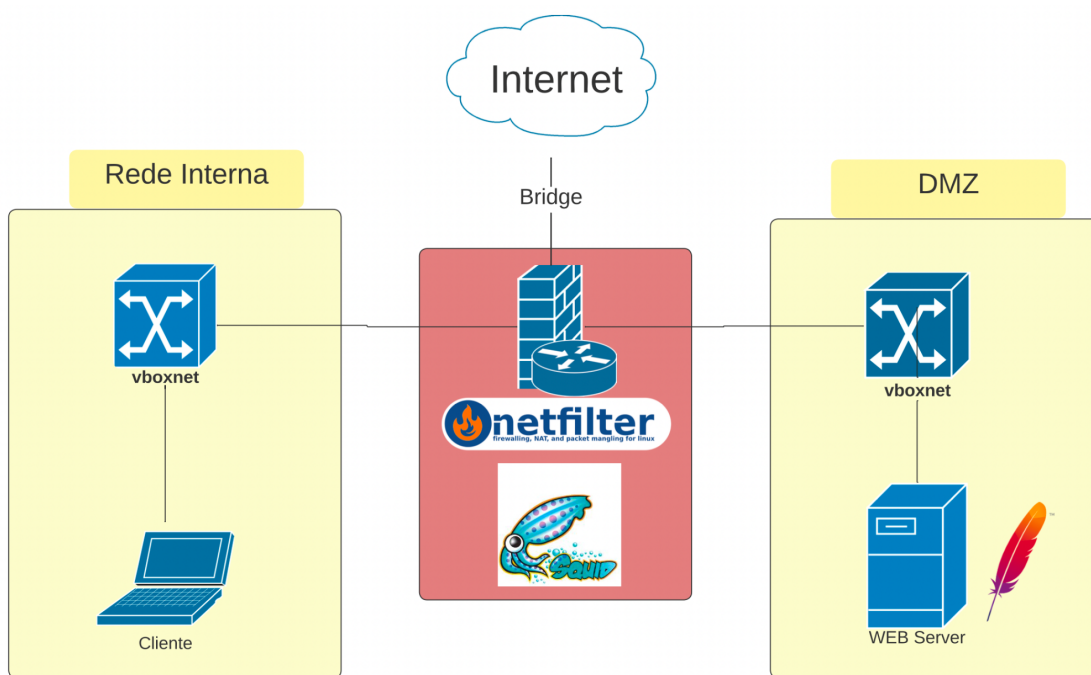


Figura 1: Cenário de Rede da organização

A organização possui duas redes diferentes que estão conectadas à Internet via firewall/router. Temos as seguintes entidades participantes:



UNIVERSIDADE
FEDERAL DO CEARÁ
Campus de Quixadá

- **Firewall/Roteador:** Consiste no roteador de borda da organização que realiza os seguintes serviços:
 - Roteamento
 - Filtro de pacotes stateful (iptables)
 - NAT (iptables)
 - Proxy HTTP/HTTPS (Squid).
- **LAN Cliente:** consiste na rede interna da organização
- **LAN DMZ:** rede para acesso externo
 - Servidor WEB: hospeda o site da organização

A seguir seguem as características que devem ser implementadas:

- Firewall/Roteador de borda
 - **Filtro de Pacotes Stateful (iptables/netfilter)**
 - Política padrão DROP.
 - Regras para o próprio firewall
 - Permitir SSH e ICMP ao firewall
 - Permitir que o firewall faça consultas DNSs
 - Regras para rede DMZ
 - Permite: HTTP, HTTPS e ICMP destinados ao Servidor Internet (LAN DMZ).
 - Regras para rede cliente
 - Permite: SSH, DNS, HTTP/HTTPS, FTP, SMTP e ICMP
 - NAT
 - SNAT: Rede interna → Internet
 - DNAT: Internet → DMZ
 - DNAT: Iptables → Squid
 - **Proxy HTTP (Squid)**
 - blacklist : domínios escolhidos pelo aluno
- Servidor Internet
 - Fornecer acesso ao site da organização via apache2

Observação: Fica a cargo das equipes a definição dos endereços IPs das redes.

Sugestão: O cenário pode ser feito no virtualbox com VMs cliente/servidor como trabalhado em laboratório.