INFRAESTRUTURA SEGURA: Armazenamento Protegido com Firewall e Monitoramento de Intrusões

INTRODUÇÃO

- O NAS ("Network Attached Storage") é um sistema de armazenamento conectado à rede.
- Nosso projeto implementa um NAS seguro, com firewall e monitoramento de acessos.
- Utilização de TrueNAS para armazenamento, IPTables/pfSense para firewall e Snort/Suricata para IDS.



ESTRUTURA DO PROJETO



PC1: NAS (TrueNAS) – Servidor de armazenamento.

- Armazena todos os arquivos do usuário.
- Permite acesso via protocolos SMB, NFS, FTP
- Gerencia permissões de usuários.
- Interface web para administração.



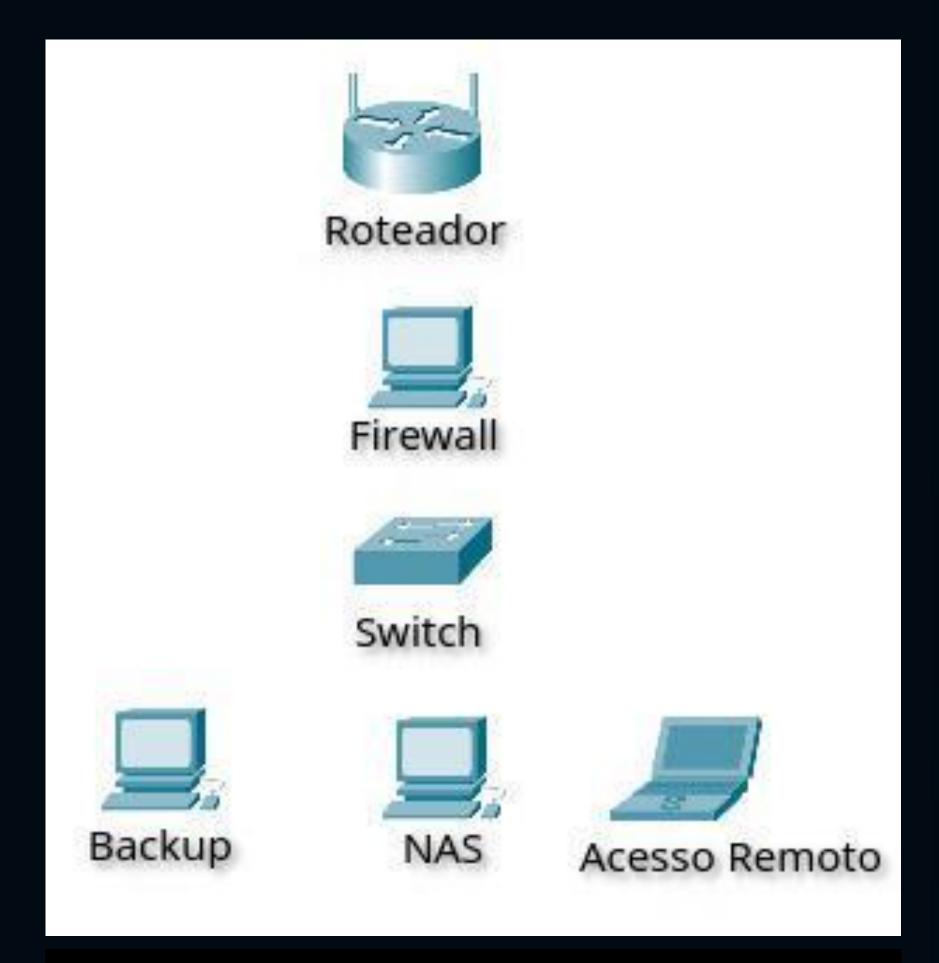
PC2: Firewall – Proteção e monitoramento de acessos.

- Controla e monitora acessos à rede.
- Utiliza pfSense/OPNsense para firewall.
- Implementa Snort/Suricata para detecção de intrusão.
- Gera logs detalhados de acessos e eventos suspeitos.



PC3: Backup – Sistema redundante para segurança.

- Mantém cópias de segurança dos dados do NAS.
- Utiliza ferramentas como rsync, BorgBackup, ZFS replication.
- Previne perda de dados em caso de falhas.



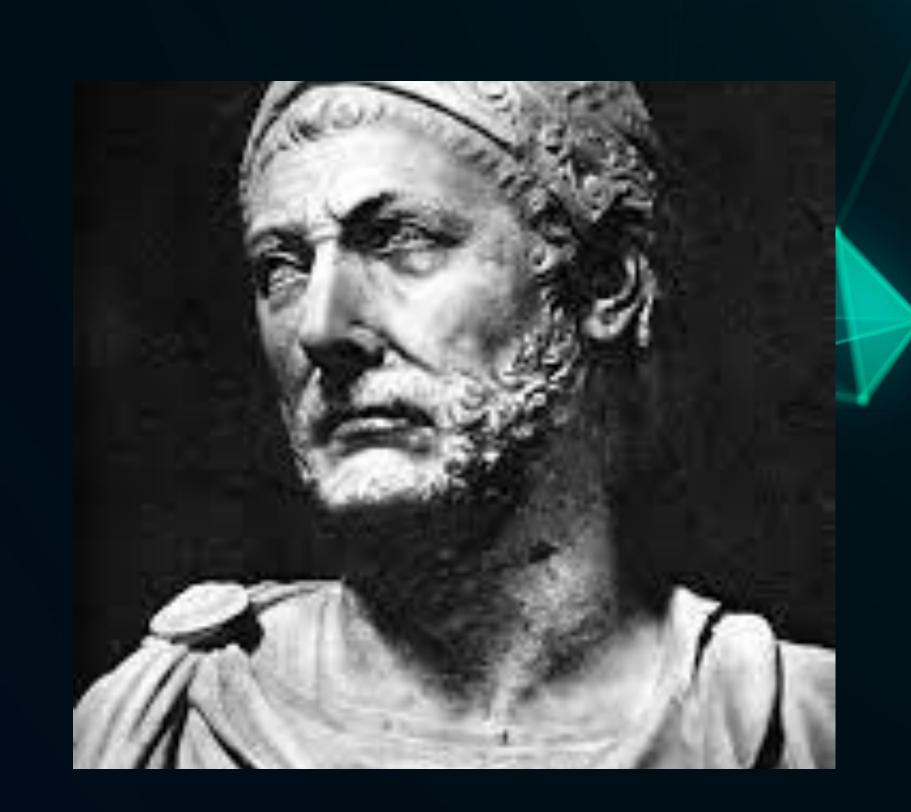
Ferramenta utilizada: Cisco Packet Tracer

DESCRIÇÃO DA CONEXÃO

- Roteador: Conecta a rede externa
 (Internet) e distribui conexão interna.
- 2. Firewall: Protege a rede filtrando tráfego de entrada e saída.
- 3. Switch: Distribui conexão entre os dispositivos internos.
- 4. NAS: Armazena e compartilha dados na rede.
- 5. Backup: Mantém cópias de segurança dos arquivos do NAS.
- 6. Acesso Remoto: Qualquer dispositivo autorizado pode acessar os dados via rede local ou VPN.



OU NÓS
ENCONTRAMOS UM
CAMINHO OU ABRIMOS
UM.
ANIBAL



OBRIGADA! PELA ATENÇÃO