Universidade Federal do Ceará – Campus de Quixadá

Disciplina: Segurança da Informação - 2017.1

Prof. Marcos Dantas Ortiz (mdo@ufc.br)

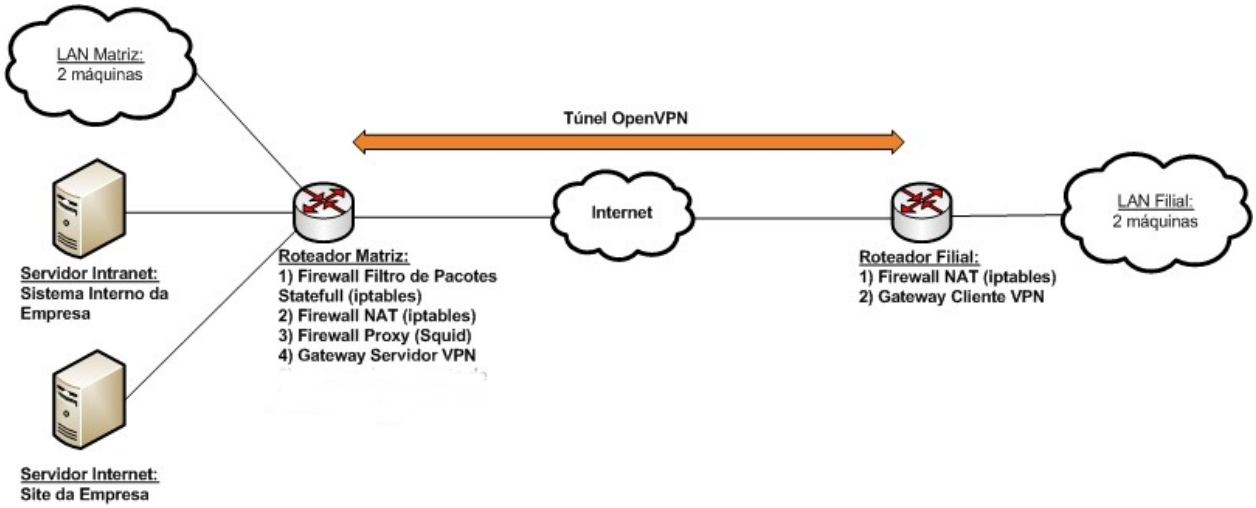
Trabalho Rede Segura

Informações importantes:

- **valor: Segunda Avaliação Parcial**
- **equipe:** 2 alunos
- **Datas importantes**
  - **entrega: dia 07/07 via SIPPA.**
    - **Documentação(parte lógica – topologia + configurações)**
    - **Apresentação: 7 de Julho**

Descrição Geral:

O objetivo desse trabalho consiste em implementar uma topologia de rede segura para uma Empresa X, com Matriz e Filial distantes geograficamente. A topologia deve ser criada utilizando um emulador e pode ser visualizada abaixo.



Aqui temos duas redes diferentes que pertencem à mesma Empresa X e estão conectadas utilizando a infraestrutura pública da Internet, pelos roteadores de borda Matriz e Filial. Temos as seguintes entidades participantes:

- **Roteador Matriz**: Consiste no roteador de borda da matriz que realiza os seguintes serviços: roteamento, filtro de pacotes stateful (iptables), NAT (iptables), Proxy HTTP (Squid) e um servidor OpenVPN.

- **Roteador Filial**: É o roteador de borda da filial, que implementa os seguintes serviços: roteamento, NAT, cliente OpenVPN.
- **LANs Matriz e Filial**: Consiste nas redes locais da Matriz e Filial, respectivamente. Cada LAN deve incluir pelo menos um computador.
- **Servidor Intranet**: Consiste em um servidor que provê o serviço de SSH apenas para os computadores da empresa X (matriz e filial). Acessado remotamente via VPN.
- **Servidor Internet**: Consiste em um servidor que hospeda o site da empresa, garantindo o acesso para qualquer máquina dentro ou fora da rede da empresa X.

A seguir seguem as características que devem ser implementadas:

- O Roteador Matriz e Filial devem se comunicar utilizando uma VPN definida pelo **OpenVPN** (LAN-to-LAN).
- O Roteador Matriz deve incluir um **Filtro de Pacotes Stateful (iptables)** que possui a regra padrão DROP. Além disso, da rede externa, permite apenas pacotes HTTP, HTTPS e ICMP, ambos destinados ao Servidor Internet. Por fim, permite a passagem de qualquer tipo de tráfego gerado pela da rede interna.
- O Servidor Intranet pode ser acessado somente pelas máquinas existentes nas LANs Matriz e Filial.
- O Servidor Internet pode ser acessado por qualquer máquina, fora e dentro da rede.
- O Roteador Matriz deve implementar um **Proxy HTTP (Squid)**, com uma blacklist que proíbe acesso aos sites do Facebook e Youtube, a partir da máquinas da LAN Matriz.
- O Roteador Matriz deve implementar um SNAT, para as máquinas da LAN Matriz.
- O Roteador Filial deve implementar um SNAT, para as máquinas da LAN Filial.
- Deve ser adicionado uma rota no Roteador Filial para a LAN Matriz via túnel.
- A VPN configurada deve prover os seguintes requisitos de segurança: Confidencialidade, Integridade e Autenticação. Configurar a Autoridade Certificadora no Roteador Matriz.
- A expansão da rede VPN deve ser feita usando o tutorial: https://openvpn.net/index.php/open-source/documentation/howto.html#scope

Observação: Fica a cargo das equipes a definição dos endereços IPs das redes e do túnel a ser configurado.