DOCUMENTAÇÃO COMPLETA DO PROJETO – REDE CORPORATIVA (Matriz + Filial) Servidor AD, Banco de dados e Monitoramento.

Curso Técnico em Redes de Computadores – SENAI

Documentação Final do Projeto de Conclusão de Curso (TCC)

1. FortiGate Matriz (172.16.13.24)

A unidade matriz é responsável pelo controle central da rede, autenticação de usuários, integração com o Active Directory, gerenciamento de políticas de segurança, distribuição de DHCP para VLANs locais e comunicação via IPsec com a filial.

1.1 Interfaces e VLANs configuradas

Todas as VLANs foram configuradas na **interface 5** do FortiGate matriz:

VLAN	Nome	Gateway	Função
VLAN 3	Servidores	192.168.3.1	AD, Servidor físico
VLAN 5	Colaboradores	192.168.5.1	Equipe de colaboradores
VLAN 8	TI	192.168.8.1	Equipe de T.I

Cada VLAN possui DHCP ativo, exceto a de servidores, com range: **192.168.X.2 – 192.168.X.254**.

1.2 Configuração do Túnel IPsec para Filial

Foi criado um túnel IPsec do tipo **Site-to-Site**, com as seguintes definições:

- **Peer:** FortiGate Filial (172.16.13.27)
- **Phase 1:** IKEv2

- **Autenticação:** PSK
- **Phase 2:**
    - Redes da matriz que precisam acessar a filial
    - Redes da filial que acessam a matriz

As redes incluídas:

- Matriz → 192.168.3.0/24, 192.168.5.0/24, 192.168.8.0/24
- Filial → 10.10.5.0/24, 10.10.8.0/24, 10.10.10.0/24

1.3 Integração com o Active Directory

Foi configurado um servidor LDAP para autenticação centralizada:

- **Servidor LDAP:** 192.168.3.20
- **Domínio:** trionetix.local
- **Login Identifier:** sAMAccountName
- **Bind DN:** administrador@trionetix.local

Grupos remotos criados:

- "Colaboradores_AD"
- "TI_AD"

Esses grupos foram associados às políticas de acesso internet e acesso interno.

1.4 Políticas de Firewall

Políticas entre VLANs

- TI → Acesso total
- Colaboradores → Acesso restrito a servidores necessários
- VLAN Servidores → Isolada, com liberações específicas
- Acesso da Matriz ao BD da Filial → Permitido

Políticas para Internet

- NAT ativado
- Webfilter
- Regras separadas por grupo de AD

Políticas da VPN

- Matriz ↔ Filial totalmente integradas
- Permissão para acessar o Banco de Dados na filial
- Permissão para AD autenticar usuários da filial

2. FortiGate Filial (172.16.13.27)

O firewall da filial atua como ponto remoto conectado à matriz via IPsec, recebendo autenticação, políticas e comunicação centralizada.

2.1 Interfaces e VLANs configuradas

VLANs também criadas na **interface 5 do firewall**:

VLAN	Nome	Gateway	Função
VLAN 5	Colaboradores	10.10.5.1	Equipe de colaboradores
VLAN 8	TI	10.10.8.1	Equipe de T.I
VLAN 10	Banco de Dados	10.10.10.1	Máquina Linux com DB

DHCP ativo nas VLANs com range:
10.10.X.2 – 10.10.X.254

2.2 Túnel IPsec com a Matriz

- Tunelamento ativo enviando suas 3 VLANs para a matriz
- Recebendo rotas para todas as redes da matriz
- Tráfego entre matriz ↔ filial funciona bidirecionalmente

2.3 Políticas de Firewall

- Liberação da Filial → Matriz (todas VLANs)
- Liberação somente de portas necessárias para acessar AD e BD
- TI com mais permissões
- Colaboradores com acesso filtrado à internet

Configuração Extra (configurado em ambos)

- Acesso permitido apenas para computadores autorizados. Utilizamos a regra de Mac Address.

3. Servidor Active Directory (192.168.3.20)

O servidor AD existe apenas na matriz, instalado dentro da **VLAN 3 – Servidores**.

3.1 Serviços Instalados

- **Active Directory Domain Services** (AD DS)
- **DNS Server**
- **DHCP** (opcional, mas no projeto foi usado DHCP do FortiGate)

3.2 Domínio

Trionetix.local

3.3 Organização das OUs

- OU TI
- OU Colaboradores
- OU Grupos

3.4 Grupos Criados

- TI
- Colaboradores

3.5 GPOs configuradas

- Bloqueio de painéis avançados
- Redirecionamento de pasta
- Políticas de senha
- Bloqueio de CMD e PowerShell
- Aplicação de GPOs por departamento

- Aplicação de papel de parede Trionetix Solutions

4. Servidor de Banco de Dados (Linux – 10.10.10.10)

O banco existe apenas na filial, instalado dentro da VLAN 10 – Banco de Dados.

4.1 Configurações gerais

- Debian/Ubuntu
- Serviço MySQL/MariaDB
- Porta 3306 (MySQL) liberada no FortiGate
- Usuários e permissões ajustados
- Backup automático configurado

4.2 Acesso Matriz → Filial

Foi criada uma política no FortiGate permitindo:

192.168.8.0/24 → 10.10.10.10
(Protocolo: TCP / Porta usada pelo banco)

E adicionado o tráfego na Phase 2 da VPN.

MONITORAMENTO – Zabbix e Grafana

O monitoramento do ambiente foi implementado utilizando **Zabbix** como ferramenta principal de coleta e análise de dados, e **Grafana** como camada de visualização. Neste projeto, o foco do monitoramento foi **exclusivamente o servidor Active Directory (AD)** localizado na matriz.

1. Configuração do Zabbix

Itens monitorados no servidor AD

O Zabbix foi configurado para monitorar os seguintes parâmetros:

- **Uso de CPU**
- **Uso de memória RAM**
- **Uso de disco**

- **Status dos serviços essenciais do AD**, incluindo:
    - Active Directory Domain Services (AD DS)
    - DNS Server
- **Disponibilidade e tempo de resposta via ICMP**
- **Disponibilidade do servidor via agente Zabbix**

Agente Zabbix

- Instalado diretamente na VM do AD (192.168.3.20)
- Configurado para reportar ao servidor Zabbix
- Porta padrão mantida (10050)

2. Integração com Grafana

O Grafana foi integrado ao Zabbix para criação de dashboards mais detalhados e gráficos mais visuais.

Dashboards criados:

- **Status geral do servidor AD**
- **Gráficos de uso de CPU, RAM e disco**
- **Gráfico de disponibilidade e tempo de resposta**
- **Painel de serviços do AD (AD DS, DNS)**

3. Objetivo do Monitoramento

O monitoramento foi implementado para:

- Garantir a **disponibilidade contínua** do Active Directory
- Antecipar falhas por meio de alertas de desempenho
- Facilitar análise e resolução de problemas
- Acompanhar a saúde do ambiente central de autenticação