MATERIAL DIDÁTICO - ADMINISTRAÇÃO DE REDES

Curso Completo para Administradores de Rede

ESTRUTURA DO CURSO

Este material foi desenvolvido especialmente para profissionais que desejam aprofundar seus conhecimentos em administração de serviços de rede em ambientes Linux.

MÓDULOS DO CURSO

MÓDULO 1 - PROXY E SQUID

■ Arquivo: modulo1_proxy_squid.md

Conteúdo:

• Conceitos fundamentais de Proxy

• Instalação e configuração do Squid

• ACLs (Access Control Lists)

• Proxy transparente

• Autenticação de usuários

• Bloqueio de sites

• Monitoramento com SARG

• Cache e otimização

• Troubleshooting

Tempo estimado: 8-10 horas

MÓDULO 2 - POSTFIX (SERVIDOR DE E-MAIL)

■ Arquivo: modulo2_postfix_email.md

Conteúdo:

• Conceitos de MTA, MDA, MUA

• Protocolos: SMTP, POP3, IMAP

• Instalação do Postfix

• Configuração básica e avançada

• Aliases e domínios virtuais

• Autenticação SASL

• Relay SMTP (Gmail)

• Segurança: SPF, DKIM, DMARC

• Anti-spam

• Troubleshooting

Tempo estimado: 10-12 horas

MÓDULO 3 - VPN (VIRTUAL PRIVATE NETWORK)

■ Arquivo: modulo3_vpn.md

Conteúdo:

• Conceitos de VPN

• Tipos: Remote Access, Site-to-Site

• OpenVPN

• Instalação e PKI

• Configuração servidor/cliente

• Certificados

• WireGuard

• Instalação

• Configuração moderna

• Performance

• IPSec/L2TP

• Troubleshooting

• Monitoramento

Tempo estimado: 12-15 horas

MÓDULO 4 - SERVIDORES WEB (APACHE E NGINX)

■ Arquivo: modulo4_servidores_web.md

Conteúdo:

• Conceitos de servidores web

• Apache

• Instalação

• Virtual Hosts

• Módulos

• .htaccess

• Nginx

• Instalação

• Server Blocks

• Proxy reverso

• SSL/TLS com Let's Encrypt

• Certificados manuais

• Headers de segurança

• Performance e otimização

• Monitoramento

Tempo estimado: 10-12 horas

MÓDULO 5 - QoS, ACLs E NAT

■ Arquivo: modulo5_qos_acls_nat.md

Conteúdo:

• QoS (Quality of Service)

• Conceitos

• Traffic Control (TC)

• HTB (Hierarchical Token Bucket)

• Priorização de tráfego

• Wondershaper

• ACLs (Access Control Lists)

• iptables

• Regras de firewall

• Proteção contra ataques

• NAT (Network Address Translation)

• Masquerade (SNAT)

• Port Forwarding (DNAT)

• NAT 1:1

• Scripts integrados

• Monitoramento

Tempo estimado: 12-15 horas

OBJETIVOS DE APRENDIZAGEM

Ao concluir este curso, você será capaz de:

■ Configurar e administrar servidores Proxy (Squid)

■ Implementar servidores de e-mail corporativos (Postfix)

■ Criar e gerenciar VPNs seguras (OpenVPN e WireGuard)

■ Administrar servidores web (Apache e Nginx)

■ Implementar QoS para priorizar tráfego

■ Criar ACLs e políticas de segurança

■ Configurar NAT e Port Forwarding

■ Realizar troubleshooting avançado

■ Monitorar e otimizar serviços de rede

PRÉ-REQUISITOS

Conhecimentos Necessários:

• Linux básico (comandos, estrutura de diretórios)

• Redes básicas (TCP/IP, DNS, DHCP)

• Noções de segurança

• Editor de texto (nano, vim)

Ambiente Recomendado:

• Ubuntu Server 20.04+ ou Debian 11+

• Mínimo 2GB RAM

• 20GB disco

• Acesso root/sudo

• Conexão com Internet

Software:

• Máquina virtual (VirtualBox, VMware) ou servidor dedicado

• Cliente SSH (PuTTY, Terminal)

• Navegador web para testes

METODOLOGIA DE ESTUDO

Recomendações:

Sequencial: Siga os módulos em ordem

Prática: Execute todos os comandos em ambiente de teste

Exercícios: Complete os exercícios ao final de cada módulo

Anotações: Documente suas configurações

Laboratório: Monte um lab com VMs

Estrutura de Cada Módulo:

• Teoria e conceitos

• Exemplos práticos

• Comandos essenciais

• Troubleshooting

• Exercícios

• Resumo

LABORATÓRIO SUGERIDO

Topologia Básica:

```
Internet
```

```
    |
[Servidor Gateway/Firewall]
    |
    ■■■ [Servidor Web - Apache/Nginx]
    |
    ■■■ [Servidor E-mail - Postfix]
    |
    ■■■ [Servidor VPN - OpenVPN/WireGuard]
    |
    ■■■ [Servidor Proxy - Squid]
```

VMs Recomendadas:

• **VM1:** Gateway (Firewall, NAT, QoS)

• **VM2:** Web Server

• **VM3:** Mail Server

• **VM4:** VPN Server

• **VM5:** Proxy Server

• **VM6:** Cliente (testes)

DISTRIBUIÇÃO DE CARGA HORÁRIA

CERTIFICAÇÃO (SUGESTÃO)

Após completar todo o material:

■ Complete todos os exercícios

■ Monte laboratório completo

■ Documente suas configurações

■ Crie casos de uso reais

■ Pratique troubleshooting

RECURSOS ADICIONAIS

Documentação Oficial:

• Squid: http://www.squid-cache.org/

• Postfix: http://www.postfix.org/

• OpenVPN: https://openvpn.net/

• WireGuard: https://www.wireguard.com/

• Apache: https://httpd.apache.org/

• Nginx: https://nginx.org/

Ferramentas Úteis:

• iptables: https://netfilter.org/

• TC (Traffic Control): https://man7.org/linux/man-pages/man8/tc.8.html

• Let's Encrypt: https://letsencrypt.org/

FLUXO DE APRENDIZADO

```
Início
  ↓
Módulo 1 (Proxy/Squid) → Exercícios
  ↓
Módulo 2 (E-mail/Postfix) → Exercícios
  ↓
Módulo 3 (VPN) → Exercícios
  ↓
Módulo 4 (Web Servers) → Exercícios
  ↓
Módulo 5 (QoS/ACL/NAT) → Exercícios
  ↓
Integração de Todos os Módulos
  ↓
Projeto Final (Laboratório Completo)
  ↓
Conclusão
```

AVISOS IMPORTANTES

Ambiente de Teste: Sempre pratique em ambiente controlado

Backup: Faça backup antes de mudanças críticas

Documentação: Documente todas as configurações

Segurança: Nunca use senhas fracas em produção

Atualizações: Mantenha sistemas atualizados

DICAS DE SUCESSO

■ Pratique cada comando antes de avançar

■ Use máquinas virtuais para experimentar

■ Consulte logs quando algo falhar

■ Teste em ambiente isolado primeiro

■ Mantenha anotações organizadas

■ Participe de comunidades online

■ Leia documentação oficial

SUPORTE

Este é um material de estudo autodidata. Para suporte adicional:

• Fóruns oficiais das ferramentas

• Stack Overflow

• Reddit: r/sysadmin, r/linux

• Comunidades Linux Brasil

CHECKLIST DE CONCLUSÃO

Ao final do curso, você deve ser capaz de marcar:

• [ ] Configurar Squid Proxy com autenticação

• [ ] Bloquear sites e categorias de conteúdo

• [ ] Instalar e configurar Postfix

• [ ] Implementar SPF, DKIM e DMARC

• [ ] Criar servidor OpenVPN funcional

• [ ] Configurar WireGuard

• [ ] Hospedar múltiplos sites em Apache

• [ ] Configurar Nginx como proxy reverso

• [ ] Obter certificados SSL Let's Encrypt

• [ ] Implementar QoS com priorização

• [ ] Criar ACLs com iptables

• [ ] Configurar NAT e Port Forwarding

• [ ] Realizar troubleshooting em todos os serviços

PRÓXIMOS PASSOS

Após dominar este conteúdo:

Estude tópicos avançados:

• Kubernetes

• Docker

• Ansible/Puppet

• Monitoramento (Zabbix, Nagios)

Certificações:

• LPIC-2

• RHCE

• CompTIA Linux+

Especializações:

• Segurança (Firewall, IDS/IPS)

• Cloud (AWS, Azure, GCP)

• DevOps

LICENÇA E USO

VERSÃO

Versão: 1.0

Data: 2024

Autor: Material Didático para Administradores de Rede

Última Atualização: Fevereiro 2024

FEEDBACK

Encontrou algum erro ou tem sugestões?

Contribua com melhorias para este material!

BOA SORTE NOS ESTUDOS! ■

Lembre-se: A prática leva à perfeição!
