Escola
Politécnica
e de Artes

Empresa fictícia com implementação de Proxy

AED - Segurança de Sistemas e Aplicações

Jefferson Ruan Teles de Oliveira
João Victor Andrade de Aquino Saraiva
Maicon Breno de Souza e Silva
Marcos Roberto de Melo Junior

Introdução da AED

Criação de uma Empresa Fictícia

- Detalhar topologia de rede
- Estabelecer uma Política de Segurança
- Implementar mecanismo de segurança - **PROXY**

Identificadas vulnerabilidades no ambiente fictício e propostas contramedidas de acordo com a norma ABNT NBR 17.799

Criação da Empresa Fictícia

Setor:

Educação

Colégio Alpha
Ensino Médio

Número de Funcionários:

60

- 20 - Administrativos
- 30 - Professores
- 10 - Técnicos

Estrutura:

Unidade única, salas de aula equipadas com laboratórios e acesso à internet

Criação da Empresa Fictícia

Colégio Alpha
Ensino Médio

Recursos de Infraestrutura:

- Data Center Local
- Rede de Lan Segmentada
- Firewall Corporativo
- Servidor **Proxy** Dedicado

Topologia da Rede

Visão Geral e Estratégia

Assegurar **segurança**, **segmentação** e **desempenho**.

Como Estratégia de Segmentação foi utilizado **VLANs** para isolar grupos de usuários e serviços, minimizando riscos e otimizando o tráfego

Zona isolada para serviços externos, principal lar do Servidor **Proxy**.

Topologia da Rede

Segmentação da Rede Interna

A segmentação é feita para diferentes perfis de usuários e serviços.

A rede é organizada no modelo de topologia **estrela** em torno de um **switch central** que serve como ponto de conexão principal para os demais equipamentos e segmentos.

4 VLANs:

Plano de Endereçamento de IP

O roteamento entre VLANs será realizado pelo **Switch Core L3**

Estratégia Geral de Endereçamento

Rede Geral

192.168.0.0/16

Gateway Padrão

192.168.1.1

Servidor Proxy

192.168.50.10

Sub-redes por Segmento VLans

- **Administrativo** (VLAN 10): 192.168.10.0/26
- **Professores** (VLAN 20): 192.168.20.0/26
- **Alunos/Laboratórios/Wi-Fi** (VLAN 40): 192.168.40.0/22
- **Servidores** (VLAN 50): 192.168.50.0/27

Plano de Endereçamento de IP

Dispositivos e Equipamentos

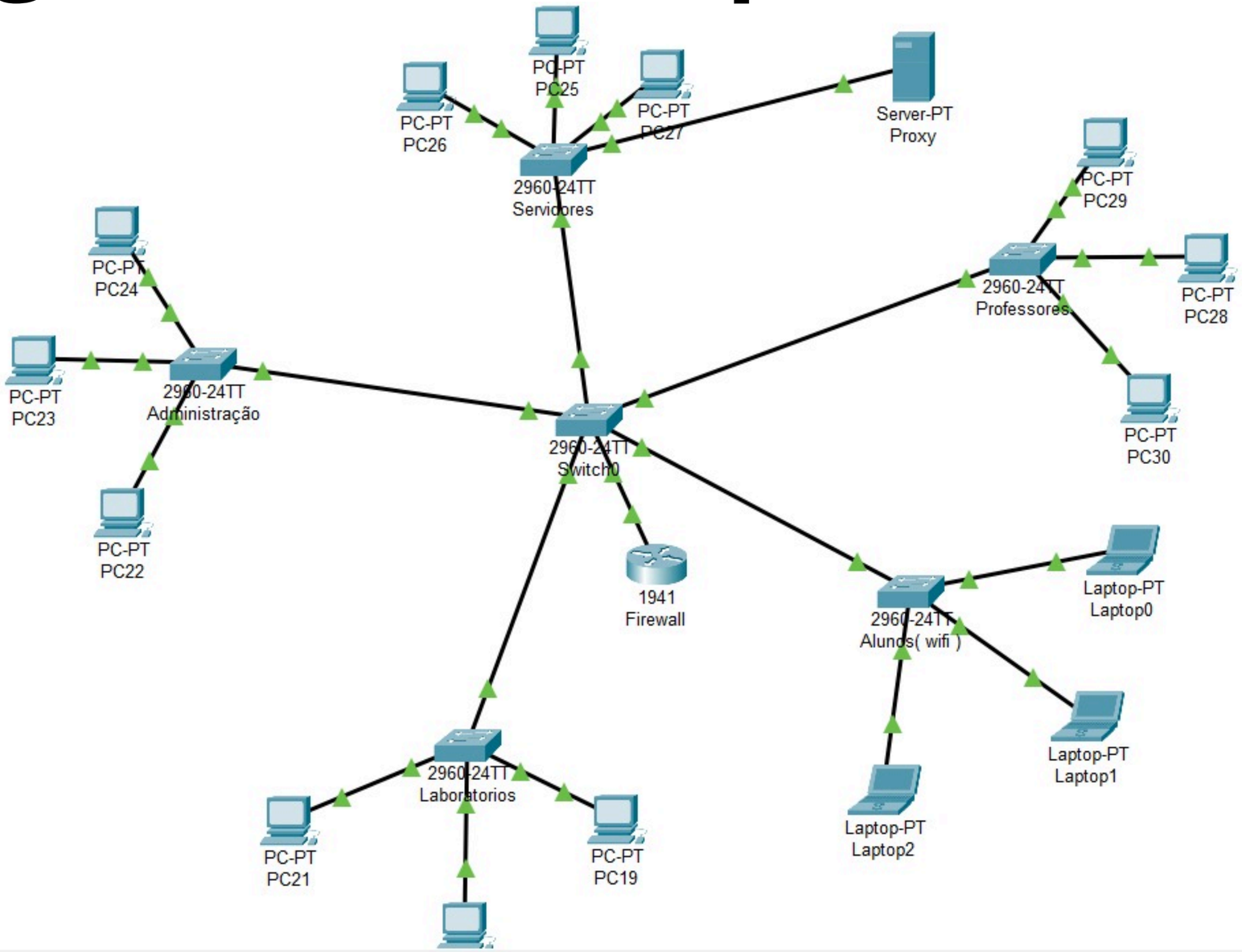
Firewall (Modelo 1941) conectado ao núcleo da rede

Switches Gerenciáveis (Modelo 2960-24TT) atuando como switch central e switches de acesso para os segmentos.

Servidor Proxy (Server-PT Proxy) localizado no segmento de Servidores

Dispositivos Finais (PCs e Laptops) conectados aos **switches** de seus respectivos segmentos (Administração, Professores, Laboratórios, Alunos Wi-Fi, Servidores)

Topologia - Rede Completa



Análise de Vulnerabilidade & Contramedidas

Visão Geral

O servidor proxy é uma ferramenta essencial para a segurança da rede do Colégio Alpha, mas não está isento de **vulnerabilidades**.

Sua posição entre os usuários e a internet o torna um alvo para **ataques**.

Esta análise foca nas vulnerabilidades mais comuns e nas contramedidas que podem ser implementadas diretamente no proxy para **mitigar os riscos**.

Análise de Vulnerabilidade & Contramedidas

Vulnerabilidade

- Interceptação de Dados Sensíveis → **Risco:** Captura de informações confidenciais
  Contramedida: Forçar o uso de HTTPS
- Uso Malicioso por Atacantes → **Risco:** Mascarar origem de ataques
  Contramedida: Implementar autenticação forte
- Problemas de Conectividade → **Risco:** Falhas no serviço
  Contramedida: Realizar manutenção
- Ataques de Força Bruta → **Risco:** Tentativas de adivinhar credenciais
  Contramedida: Bloquear múltiplas tentativas de login falhas

Análise de Vulnerabilidade & Contramedidas

Vulnerabilidade

Propagação de Malware → **Risco:** Pode se tornar ponto de entrada para malware
Contramedida : Atualizar as políticas de filtragem

Políticas de Filtragem Inadequadas → **Risco:** Regras de bloqueio mal definidas
Contramedida: Definir políticas de filtragem claras

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ABNT NBR 17.799)

“O uso não pedagógico de dispositivos digitais no ambiente escolar, em qualquer etapa de ensino, pode trazer prejuízos para o processo de aprendizagem e desenvolvimento de crianças e adolescentes”

CRIANÇAS, ADOLESCENTES E TELAS GUIA SOBRE USOS DE DISPOSITIVOS DIGITAIS

-Governo Federal

Pensando nisso foi desenvolvido a seguinte Política de Segurança:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ABNT NBR 17.799)

Objetivos Gerais:

Preservação da **integridade**, **disponibilidade** e **confidencialidade**

Proteção da Comunidade Escolar, resguardando os alunos, professores e funcionários contra os riscos digitais, incluindo acesso a conteúdo impróprio, cyberbulling, exposições a malwares e outras ameaças;

Promover o Foco Educacional, assegurando que os recursos tecnológicos, especialmente o acesso à internet, sejam utilizados prioritariamente para fins pedagógicos, minimizando distrações e otimizando o tempo de estudo e pesquisa;

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (ABNT NBR 17.799)

Objetivos Gerais:

Garantir a Segurança da Infraestrutura, o qual irá proteger a rede, os sistemas e os equipamentos do Colégio Alpha Ensino Médio contra acessos não autorizados, danos, interrupções e uso indevido;

Assegurar a Conformidade Legal e Ética, garantindo que o uso da tecnologia esteja em conformidade com a lesgilação vigente (LGPD) e com os princípios éticos e valores do Colégio Alpha.

CONFIGURAÇÃO DO PROXY

Ferramenta Utilizada

Squid, um servidor proxy em uma máquina virtual.

Principais Implementações

- Listas de Controle de Acesso (ACLs)
- Autenticação de Usuários
- Registro de Logs
- Monitoramento

Resultado

Ao acessar a internet, o usuário precisa fornecer credenciais válidas, garantindo que apenas membros da comunidade escolar utilizem a rede. O acesso é negado caso o usuárionão possua um cadastro.

CONFIGURAÇÃO DO PROXY

```
# Autenticação
auth_param basic program /usr/lib/squid/basic_ncsa_auth /etc/squid/passwd
auth_param basic realm Escola_Proxy
acl autenticados proxy_auth REQUIRED

# Grupos
acl professores proxy_auth "/etc/squid/professores"
acl alunos proxy_auth "/etc/squid/alunos"
acl adm proxy_auth "/etc/squid/adm"

# Sites bloqueados para alunos e professores
acl sites_bloqueados dstdomain .facebook.com .instagram.com .youtube.com


# Políticas de acesso
http_access deny professores sites_bloqueados
http_access allow professores
http_access deny alunos sites_bloqueados
http_access allow alunos
http_access allow adm
http_access allow autenticados
http_access deny all
#acessos de log
access_log /var/log/squid/access.log squid
cache_log /var/log/squid/cache.log
logfile_rotate 10
```

CONCLUSÃO

A implementação do proxy, apoiada pela segmentação da rede em VLANs e por políticas de segurança, protege os ativos de informação da escola e os dados de alunos e funcionários

Para garantir a eficácia contínua, recomenda-se a monitorização constante do ambiente, a atualização dos sistemas e a revisão periódica das listas de controle do **proxy**.

Escola
Politécnica
e de Artes

Obrigado !

Empresa fictícia com implementação de Proxy

AED - Segurança de Sistemas e Aplicações

Jefferson Ruan Teles de Oliveira
João Victor Andrade de Aquino Saraiva
Maicon Breno de Souza e Silva
Marcos Roberto de Melo Junior