

Apresentação sobre SecOps em ambiente controlado

Bem-vindo a esta apresentação técnica. Neste guia, abordaremos tópicos cruciais para profissionais de segurança da informação, incluindo hardening de contas de serviço, autenticação PKI, design de infraestrutura de rede segura, mitigação de vulnerabilidades e resolução de problemas de conectividade.



Sobre mim

- Sou Gabriel Andre Sauer, tenho 25 anos.
- Comecei a aprender sobre informática logo cedo, aos 12 anos, com curso técnico de informática.
- Trabalhei na empresa dos meus pais, montando computadores dos funcionários e também implementei o Gold System, CRM de serviços funerários externo, usando um servidor Windows Server R2.
- Sou formado em Análise e desenvolvimento de sistemas pela Uniasselvi - Blumenau
- Completei diversos bootcamps sobre Cybersecurity, como por exemplo CyberSecurity - Santander Universidades e também Especialista em Segurança digital, pela [DIO.me](https://dio.me)
- Atualmente curso Pós Graduação em Cibersegurança pela PUCPR.



Apresentação teórica

1

Hardening em Contas genéricas

2

Autenticação PKI com Smart Cards

3

Processo de autenticação baseado no método PKI

4

Infraestrutura de Rede - CF como proteção de acesso

5

Mitigação da Vulnerabilidade CVE-2016-8745 no TomCat

6

Resolução de Problemas de Conectividade

7

Resolução de Problemas de Conectividade

Hardening de Contas Genéricas de Serviço

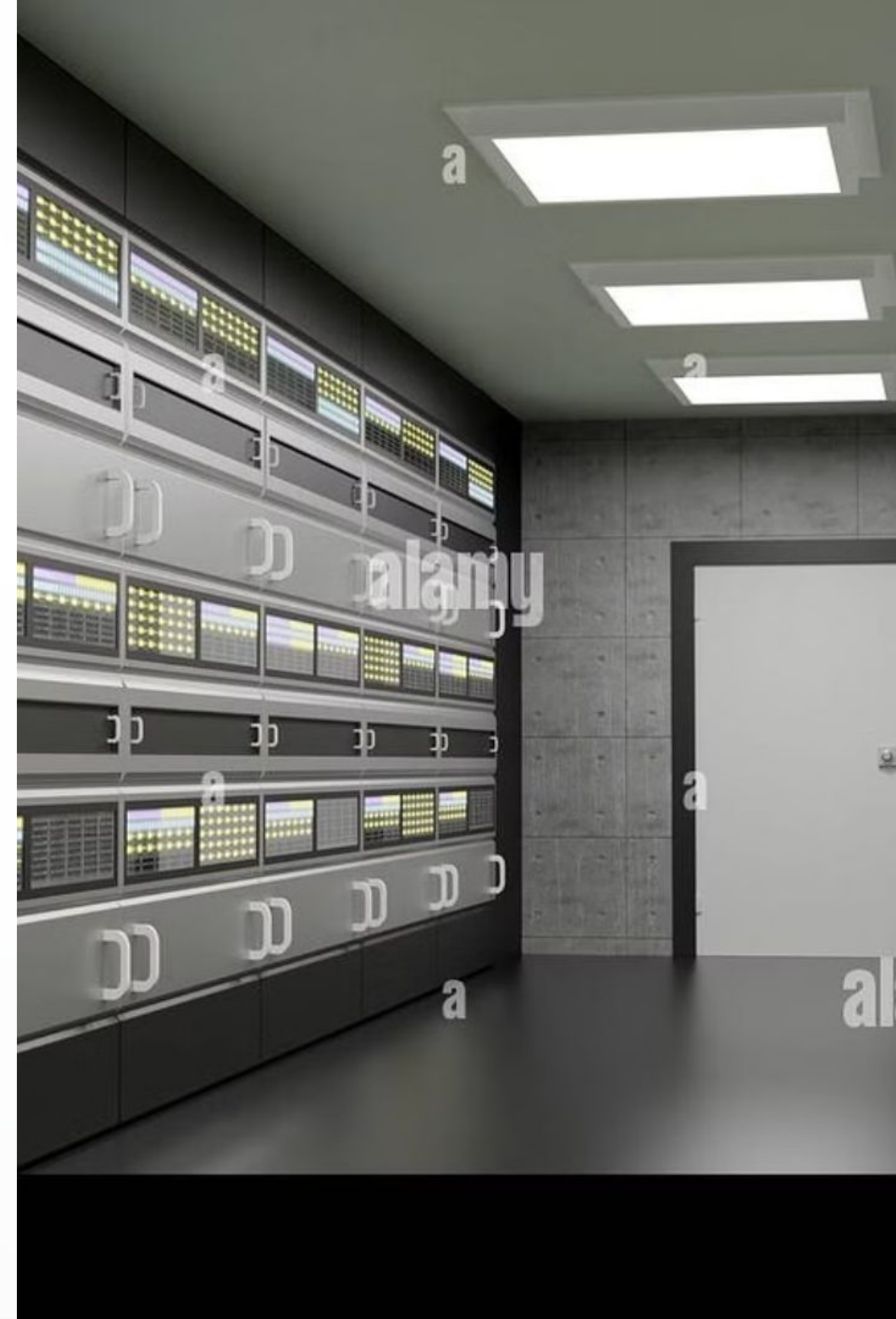
- 1 Auditoria e Inventário**

Realize um levantamento completo de todas as contas de serviço existentes, documentando suas funções e permissões.
- 2 Princípio do Menor Privilégio**

Revise e ajuste as permissões para garantir que cada conta tenha apenas os acessos estritamente necessários para sua função.
- 3 Rotação de Senhas**

Implemente um sistema de rotação automática de senhas, utilizando geradores de senhas fortes e únicas para cada conta.
- 4 Monitoramento Contínuo**

Estabeleça um sistema de monitoramento em tempo real para detectar atividades suspeitas ou anômalas nas contas de serviço.



Autenticação PKI com Smart Cards

1

Emissão do Certificado

A CA interna gera um certificado digital único para cada usuário, que é armazenado no Smart Card.

2

Autenticação do Usuário

O usuário insere o Smart Card e fornece um PIN para desbloquear o certificado.

3

Verificação do Certificado

O sistema verifica a validade do certificado com a CA interna.

4

Acesso Concedido

Se o certificado for válido, o acesso é concedido ao usuário autenticado.

Processo de autenticação baseado no método PKI

1

Geração do CA

Usuário solicita a CA a geração do par de chaves e CSR para a Certificadora interna

2

CA INTERNA

A certificadora valida o par de chaves e gera um certificado para o cliente, juntamente com o smartcard com a chave privada e um PIN de acesso

3

Servidor

Servidor recebe o certificado e armazena a chave pública do cliente, aguardando a chave privada do cliente, para descriptografar os dados

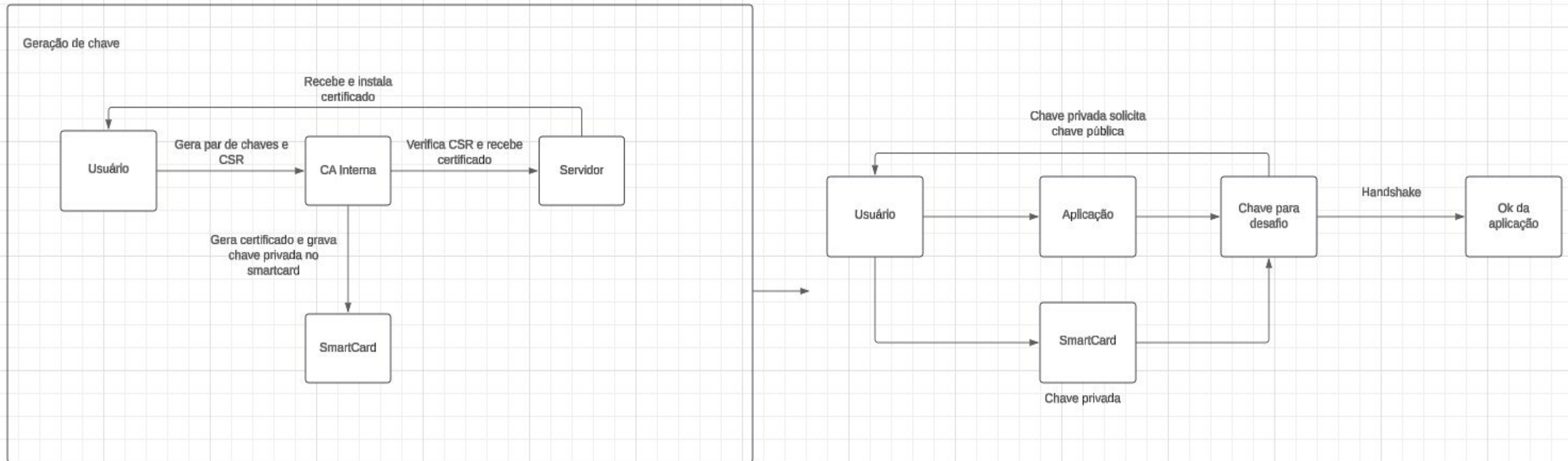
4

Conexão a aplicação

Cliente se conecta a aplicação, onde é proposto um desafio para validar a identidade.

O cliente conecta seu smart card em seu computador, usando um navegador confiável, insere seu PIN e faz a validação com o servidor, autenticando o acesso

Processo de autenticação baseado no método PKI



Infraestrutura de Rede - CF como proteção de acesso

1

Usuários

Os usuários são todos autenticados, utilizando cofre de senhas, certificados, antivírus e feito hardening, como logout automático, acesso somente autorizado e privilégios restritos

2

Filiais

Filiais possuem intranet para compartilhamento de dados entre usuários. É usado VPN para acesso a ambientes externos, além de firewall e controle de acesso as áreas restritas

5

LDAP

LDAP faz a autenticação de usuários, confirmando suas identidades e a transição de dados, protegendo por TLS cada informação enviada entre eles

3

Cloudflare

Ao se conectar ao servidor, todos os acessos das filiais passam pela Cloudflare, fazendo a limpeza da conexão e protegendo o endpoint de acessos não autorizados ou tentativa forçada de acesso, além da proteção DDoS

4

Load Balancer

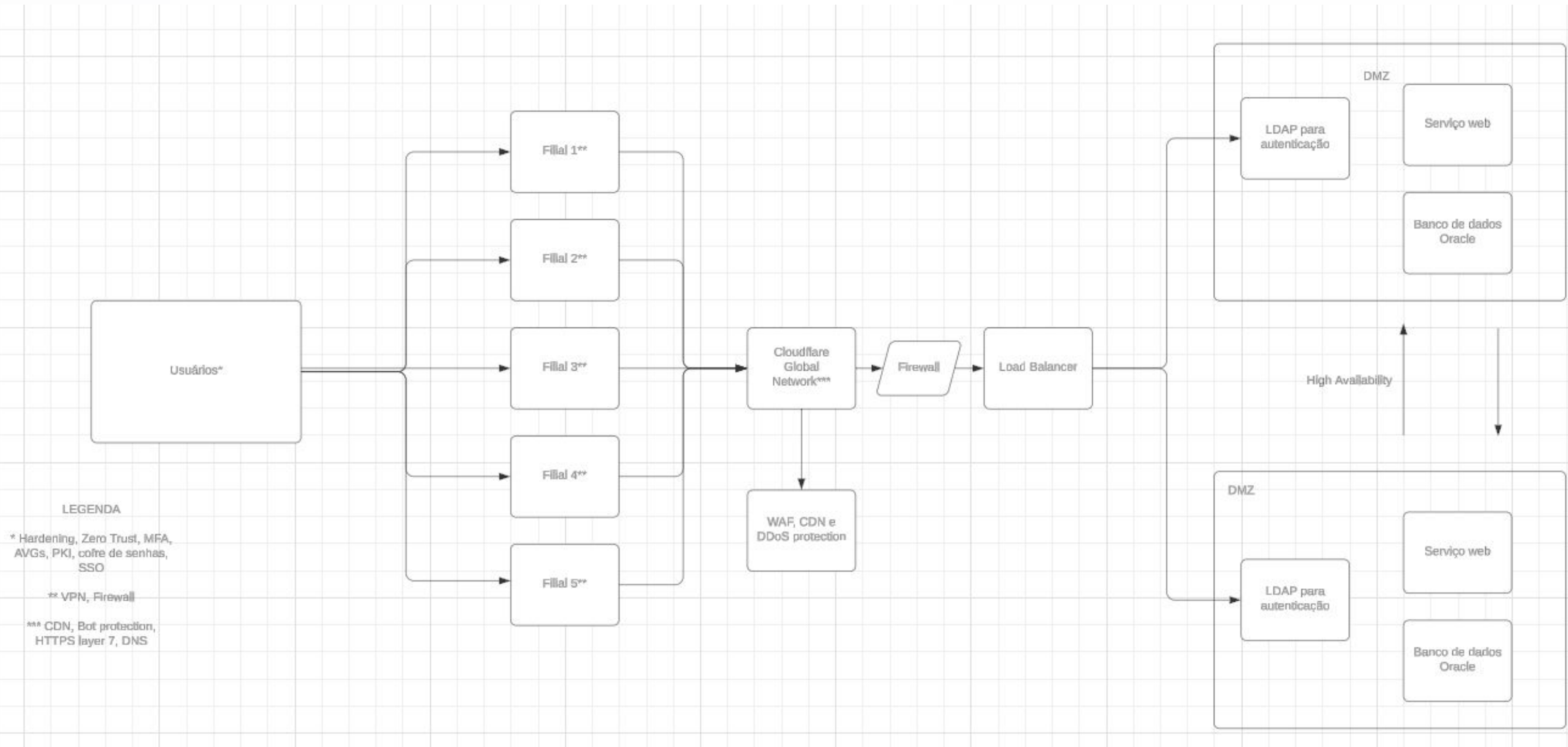
Após passar pelo WAF da CF, o usuário é designado ao servidor com melhor carga, evitando assim sobrecarga do sistema e lentidão, garantindo a disponibilidade em tempo real

4

DMZ

O serviço web quanto o banco de dados, estão sobre uma zona de segurança, protegendo contra tráfego não confiável, fazendo assim, a segurança local dos acessos

Infraestrutura de Rede - CF como proteção de acesso



Mitigação da Vulnerabilidade CVE-2016-8745 no TomCat

1

Identificação

Confirme a versão do TomCat afetada e os detalhes específicos da vulnerabilidade CVE-2016-8745.

2

Atualização

Aplique o patch de segurança mais recente fornecido pelo Apache para o TomCat, seguindo as melhores práticas de gerenciamento de mudanças.

3

Teste

Realize testes extensivos no ambiente de homologação para garantir que a atualização não cause problemas de compatibilidade.

4

Implementação

Implemente a atualização no servidor de produção durante uma janela de manutenção programada.

Step-by-step instructions for implementing a Patch Management process

1

Establish device
groups by OS and
critical status

2

Inventory all the
software in use

3

Delineate your
Patch Management
policy

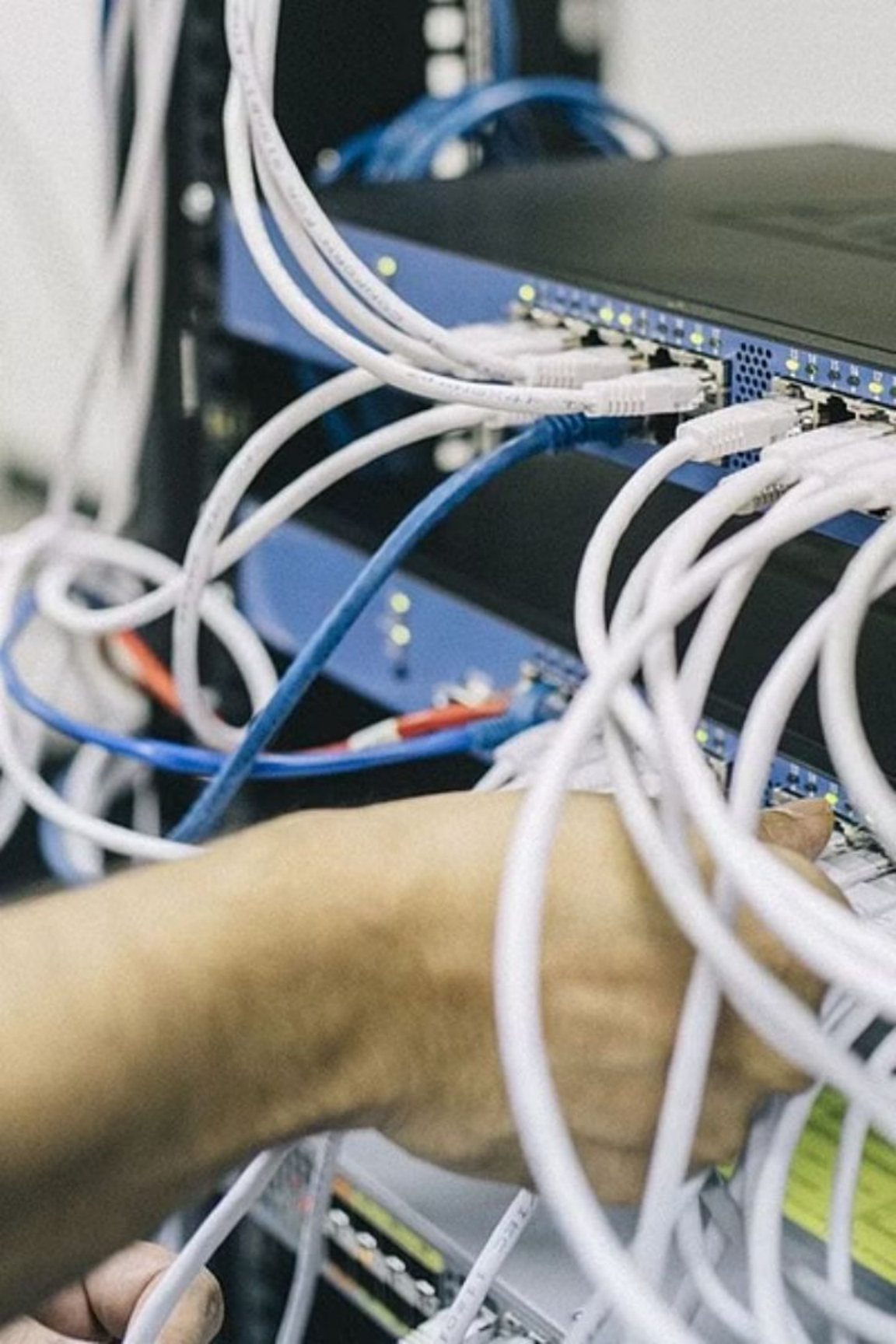
4

Find outdated
software with
InvGate Insight

5

Deploy
patches

 invgate



Resolução de Problemas de Conectividade



Análise de Rede

Use ferramentas como Wireshark para capturar e analisar o tráfego entre a workstation A e o servidor B.



Verificação de Firewall

Examine as regras do firewall usando comandos como 'iptables -L' para identificar bloqueios.



Inspeção do Servidor

Utilize 'netstat -tuln' no servidor B para verificar as portas em escuta do serviço.



Testes de Conectividade

Execute 'ping' e 'traceroute' para verificar a rota e a latência entre os dispositivos.

Ferramentas Avançadas para Diagnóstico

Nmap

Use o Nmap para fazer uma varredura de portas no servidor B: 'nmap -p-192.168.2.X' (ou outro IP local atribuído). Isso ajudará a identificar quais portas estão abertas e potencialmente em uso pelo serviço.

TCPDump

Capture pacotes na interface de rede do servidor B usando TCPDump: 'tcpdump -i eth0 -n'. Isso permitirá observar o tráfego em tempo real e identificar tentativas de conexão.

Sysinternals

Se o servidor B for Windows, use ferramentas Sysinternals como Process Monitor para rastrear atividades do sistema e identificar processos relacionados ao serviço afetado.

Conclusão e Próximos Passos

Documentação

Crie uma documentação detalhada de todos os processos, configurações e soluções implementadas durante esta análise de segurança.

Treinamento

Desenvolva um programa de treinamento para a equipe de TI, focando nas melhores práticas de segurança e nos procedimentos de resolução de problemas discutidos.

Monitoramento Contínuo

Implemente um sistema de monitoramento contínuo para detectar e responder prontamente a potenciais ameaças de segurança e problemas de conectividade.

Revisão Periódica

Estabeleça um cronograma para revisões periódicas de segurança e atualizações de infraestrutura para manter a postura de segurança atualizada.



Referências

Criação de diagramas, disponível em:

<https://lucid.app/>

High Availability Database Definition, disponível em:

<https://www.scylladb.com/glossary/high-availability-database/>

Layout do slide, disponível em:

<https://gamma.app/>

Load Balancing Reference Architecture, disponível em:

<https://developers.cloudflare.com/reference-architecture/architectures/load-balancing/>

Oracle database, disponível em:

<https://www.oracle.com/database/>

Significado de protocolo de acesso a diretório leve (LDAP), disponível em:

<https://www.fortinet.com/br/resources/cyberglossary/ldap-authentication/>