Efraim de Almeida Lima - SEGNA5

Projeto de Topologia Segura com Serviços Críticos

Arquitetura de Defesa em Profundidade - Descrição Técnica e Políticas

Seguindo as solcicitações da atividade desenvolvi o seguinte trabalho, sendo que adicionei por minha parte um servidor LDAP e outro com IAM, junto com ACLs para a parte de autenticação solicitada.

1) Descrição de Cada Elemento

Firewall

- Controla o tráfego entre zonas de rede com base em políticas de segurança (IP, portas, protocolos, aplicação).
- Implementa inspeção stateful, NAT, e pode incluir funcionalidades UTM/NGFW (IPS, Antimalware, SSL inspection, App Control).

Tipos:

- Stateful: Mantém estado de conexões; permite/nega tráfego com base em sessões e regras.
- Application Layer / NGFW: Inspeciona o conteúdo e contexto das aplicações, permite regras por aplicação/usuário, decriptografia SSL/TLS, DLP básico e WAF embutido em alguns casos.

Redundacia para evitar falhas e indisponibilidade.

IPS/NIPS (Intrusion Prevention System)

- Detecção com base em assinaturas, heurística/anomalias (estatística/comportamental), reputação (feeds), detecção de evasão (normalização de protocolo), decodificadores específicos (HTTP, SMB, DNS).

Como previne:

- O modelo inline, descarta pacotes maliciosos, reseta sessões, bloqueia hosts por tempo (shunning), aplica rate limiting dinâmico.
- Integra com firewall para atualização de objetos dinâmicos (endurecimento adaptativo).

Boas práticas:

- Modo de aprendizagem em produção controlada antes de "block".
- Regras por zona/serviço para reduzir falsos positivos.
- Atualizações frequentes de assinaturas e tuning contínuo.

DMZ (Demilitarized Zone)

Importância:

- Isola serviços expostos à Internet da rede interna, reduzindo movimento lateral.
- Permite políticas mais restritivas entre DMZ ↔ Interno do que Internet ↔ DMZ.

Serviços típicos na DMZ:

- Web front-ends, reverse proxies, WAF (se não acoplado ao LB), servidores de e-mail (gateway/relay), DNS autoritativo externo, bastion hosts para saltos controlados.

Integrações:

- HIDS/HIPS/EDR nos servidores DMZ.
- Logs enviados a SIEM; controle estrito de egress (por exemplo, apenas para APIs ou bancos em portas específicas via firewall interno).

VPN Concentrator

Como garante acesso remoto seguro:

- Túneis IPsec/SSL VPN com criptografia forte (AES-GCM), PFS, e renegociação periódica de chaves.
- Autenticação forte via IAM/LDAP (MFA, certificados clientes, SAML/OIDC para ZTNA).
- Políticas de split-tunnel conforme necessidade; postura do endpoint (NAC/host-check) antes de conceder acesso.
- Segmentação: usuários VPN entram em VLAN/VRF própria com ACLs e regras de microacesso (just-in-time quando possível).

Proxy Server
Controle de acesso e filtragem:
- Proxy HTTP/HTTPS com autenticação integrada ao LDAP/IAM (transparent ou explicit).
- Filtragem por categorias (URL filtering), reputação, bloqueio de malware/phishing, DLP básico na saída.
- TLS intercept/SSL inspection com exceções para privacidade/compliance.
- Logs detalhados (URL, usuário, ação) enviados ao SIEM; políticas por grupo (ex.: devs, finanças).

Anti-DDoS
Como mitiga ataques volumétricos:
- Camada upstream (provedor/cloud scrubbing) para absorver volumetria L3/L4 (SYN flood, UDP flood).
- Técnicas: rate limiting com base em ASN/IP, detecção de anomalias de baseline, challenge/response (CAPTCHA/JS), validação de protocolo.
- Integração com BGP FlowSpec/RTBH para desvio e mitigação fora do data center.
- Telemetria para SIEM e ajuste em tempo real via SOC.

Segmentação (VLANs/VRFs/Microsegmentação)
Benefícios para segurança interna:
- Limita movimento lateral e escopo de incidentes.
- Implementa princípio do menor privilégio em nível de rede.
- VLANs por função (Usuários, App, DB, Gerência, VPN); VRFs para isolar domínios de roteamento.
- Microsegmentação com firewalls internos/ACLs entre workloads (leste-oeste), preferencialmente com identidades de workload (labels) quando disponível.

HIPS/EDR
Proteção em endpoints e servidores:
- HIPS: prevenção local a explorações (proteção de memória, bloqueio de execuções não autorizadas, controle de aplicações).
- EDR: telemetria avançada, detecção comportamental (MITRE ATT&CK), quarentena, coleta forense, resposta remota.
- Integra com IAM (condições de acesso baseadas em postura), SIEM (correlação) e SOAR (resposta automatizada).

Servidor de Logs/SIEM
Monitoramento e correlação:
- Centraliza logs (firewalls, IPS/IDS, WAF, LB, proxy, VPN, LDAP, IAM, servidores, EDR).
- Normalização, enriquecimento (GeoIP, TI), correlação multi-fonte, detecção de anomalias, UEBA.
- Dashboards de postura, alertas priorizados, playbooks de resposta (via SOAR).
- Retenção conforme compliance; trilha de auditoria para investigações.

Servidor de Atualizações (Patch/WSUS/Linux Repo/3rd Party)
Gestão de patches e hardening:
- Orquestra patching de SO e aplicativos (também firmware de rede/segurança).
- Janelas de manutenção e anéis de implantação (canary → broad).
- Baseia-se em CIS Benchmarks/NIST para hardening; varredura de compliance pós-patch.
- Integra com EDR para validação de versão/assinatura e com SIEM para auditoria.

LDAP Server (Diretório) e IAM
Diretório LDAP:
- Armazena identidades, grupos, atributos e políticas que são consumidos por VPN, Proxy, servidores, aplicativos.
- Alta disponibilidade (multi-master/replicação), TLS obrigatório, bind seguro e controles de schema.
- IAM:
- MFA, SSO (SAML/OIDC), JIT/JEA, RBAC/ABAC, rotinas de provisionamento/desprovisionamento.

- Governa acesso administrativo (break-glass), revisões periódicas (access reviews) e logs de autenticação para SIEM.

Load Balancer com WAF integrado
Funções combinadas:
- Distribuição de tráfego (L4/L7), health checks, SSL offloading, session stickiness.
- WAF: regras para OWASP Top 10 (SQLi, XSS, CSRF), validação de cabeçalhos, rate limiting por caminho/API, bot management.
- Integração com IDS/IPS e SIEM; bloqueio dinâmico por assinaturas e reputação.

Servidor com ACLs
Papel:
- ACLs no SO e no filesystem (POSIX/NTFS) para controlar acesso a pastas/dados sensíveis por grupo/função (via LDAP/IAM).
- ACLs de rede (host-based firewall) para restringir portas de gestão e serviços internos.
- Auditoria habilitada (file access audit) com envio ao SIEM.

2) Políticas de Segurança - Exemplos Práticos
Regras de Firewall (Entrada/Saída)
- Perímetro (Internet → DMZ):
  - Permitir apenas portas necessárias por serviço (ex.: 80/443 para web; 25/587 para SMTP relay; 53/UDP/TCP para DNS autoritativo).
  - Bloquear todo o restante (deny-all implícito).
  - Aplicar inspeção TLS no NGFW onde permitido, e política WAF no LB.
- DMZ → Interno:
  - Web front-ends na DMZ só podem acessar backends internos específicos (ex.: App API na porta 8443/TLS; DB via proxy/jump apenas quando arquiteturalmente necessário).
  - Bloquear conexões iniciadas da rede interna para a Internet via portas não aprovadas (egress filtering). Proxy obrigatório para HTTP/HTTPS.
- Gerência (VLAN Mgmt):
  - Acesso somente via jump/bastion, com MFA e IPs permitidos.
  - Bloquear acesso lateral entre dispositivos de rede (no mesh), exceto protocolos de gestão controlados (SSH v2, SNMPv3, NTP, syslog TLS).
- VPN:
  - Usuários VPN entram em subnet dedicada; acesso somente a recursos específicos via ACLs (Zero Trust).
  - Proibir tráfego leste-oeste entre clientes VPN.
- Saída (Egress):
  - Bloquear 25/TCP (SMTP) externo, exceto relays aprovados.
  - Restringir saída para 80/443 somente via proxy/Firewall com inspeção.
  - Bloquear DNS direto para Internet; obrigar uso de DNS interno/seguro.

Controle de Acesso entre VLANs
- VLAN Usuários → VLAN App:
  - Permitir apenas portas das aplicações publicadas (ex.: 443/TLS); negar SMB/WinRM/RDP direto.
- VLAN App → VLAN DB:
  - Permitir somente portas do banco (ex.: 5432/3306/1433) e somente entre hosts concretos (objeto de rede) ou através de proxies.
  - Implementar TLS mútua entre app e DB quando possível.
- VLAN Mgmt:
  - Isolada; acesso apenas de jump hosts e contas de administração com MFA.
- VLAN VPN:
  - Regras específicas por grupo (RBAC de rede): por exemplo, "Suporte" pode acessar RDP/SSH de jump; "Vendas" apenas porta 443 de aplicações internas.
- IDS/IPS interno entre zonas com políticas distintas para detectar lateral movement.

Autenticação Forte na VPN (MFA)
- Requisitos:
  - MFA obrigatório (TOTP, push, FIDO2) + senha complexa/rotacionada.
  - Opcional/fortemente recomendado: certificados de cliente instalados e vinculados ao dispositivo.
  - Postura do endpoint: EDR instalado, disco criptografado, firewall local ativo, patches dentro do baseline.
- Fluxo:
  - Autenticação primária no IAM (SAML/OIDC/LDAP bind seguro).
  - Autorização baseada em grupos/atributos (ABAC) para mapear políticas de rede (atribui VLAN/ACLs dinâmicas).
- Sessões:
  - Idle/absolute timeout definidos; reautenticação periódica; detecção de anomalia (local incomum).

Política de Atualização e Antivírus/EDR
- Patching:
  - Sistemas críticos: patch ciclo quinzenal; emergenciais (zero-day) em 48-72h após validação.
  - Anéis: Dev/Test → Piloto → Produção; janela de manutenção definida.
  - Firmware de rede e segurança incluídos no calendário; backups antes de upgrade.
- Antivírus/EDR:
  - EDR obrigatório em servidores e endpoints com políticas "block" para técnicas MITRE mais comuns (defense evasion, credential dumping).
  - Atualizações de assinaturas e agente diárias; telemetria enviada ao SIEM.
  - Quarentena automática para IOC de alta confiança; playbooks de resposta (isolar host, coleta de artefatos, reset de credenciais).
- Hardening:
  - Baselines CIS aplicados (SO, DB, web); auditoria contínua de configuração via ferramenta de compliance.
  - Desabilitar serviços/portas desnecessários; aplicação de TLS1.2+ e chaves fortes; rotação de credenciais.

3) Integrações Recomendadas (LDAP, IAM, WAF/LB, ACLs)
- LDAP + IAM:
  - IAM como autoridade de autenticação (SSO, MFA), LDAP como fonte de grupos/atributos.
  - VPN, Proxy, WAF e aplicações integram-se ao IAM; servidores usam LDAP para autorização local (grupos) quando apropriado.
- WAF no LB:
  - Políticas por aplicação e caminho; modo "block" para regras de alta confiança; virtual patches para CVEs.
  - Rate limiting por IP/AS e por token de API; bot management básico.
- ACLs em servidores:
  - Áreas sensíveis com ACLs por grupo; habilitar "file access auditing" e enviar eventos ao SIEM.
  - Host-based firewall negando por padrão e permitindo apenas portas necessárias.

4) Itens Operacionais (SOC/SIEM)
- Logging obrigatório: firewall, WAF, IPS/IDS, VPN, Proxy, LDAP/IAM, EDR, SO, DB, aplicações.
- Alertas prioritários: múltiplas falhas de MFA, elevação de privilégio, exfiltração suspeita (alto volume para destinos incomuns), tentativas de exploração no WAF, mudanças críticas em ACLs/grupos LDAP.
- Testes e melhoria contínua: exercícios de tabletop, purple teaming, revisão trimestral de regras/assinaturas, validação de exceções no WAF/Firewall.