TLSStress.Art
SECURE CONNECTIONS. MAXIMUM PERFORMANCE.

STACK TECNOLÓGICO

NGFW · TLS DECRYPTION TEST BENCH

O TLSStress.Art é um test bench multi-vendor para validar performance de decriptografia TLS em next-generation firewalls. Este documento resume o stack tecnológico — cada camada, cada componente — e a justificativa por trás de cada escolha. Filosofia: standards-first, open-source com licenças permissivas, supply-chain hardened do primeiro commit ao deploy em produção.

TEST AGENTS 01

GERADORES DE TRÁFEGO

Playwright
Node.js + Chromium headful — único stack cobrindo H2 + H3 (QUIC) com handshake TLS real.

k6
Go — high-throughput load testing scriptável em JS, runtime compilado.

Caddy 2.8.x
Origem TLS Go — H2+H3 nativo, autoTLS, ECDHE+AEAD apenas.

cert-manager
PKI K8s-native — certs com IP SANs por VLAN.

DATA & MONITORING 02

PERSISTÊNCIA E OBSERVABILIDADE

PostgreSQL 16+
TimescaleDB-friendly, Drizzle-friendly, pgvector ready.

Drizzle ORM
TypeScript-native, type-safe; migrations SQL-first auditáveis.

Prometheus
Padrão K8s; PromQL expressivo; SLA scrape □ 15s.

Grafana + Loki
Provisionável via JSON; LogQL = PromQL-like; cost-effective.

ORCHESTRATION 03

PLATAFORMA E REDE

K3s / RKE2
K8s leve, low-overhead; airgap-friendly, LTS.

Multus + macvlan
Multi-NIC K8s; bypassa iptables nas data planes.

Velero + WAL-G
K8s backup + PostgreSQL PITR (ADR 0017).

Ansible-runner
Lib oficial AWX para SSH/Telnet vendor automation.

SUPPLY CHAIN 04

SEGURANÇA END-TO-END

Sigstore / cosign
Image signing keyless OIDC — sem chave a guardar.

Syft (SPDX)
SBOM por release; integra com cosign attestation.

Trivy + CodeQL
Vuln scan + SAST integrado ao GitHub Security.

GitHub Actions
CI multi-arch (amd64+arm64); auto-merge gated por checks.

ÍNDICE DE STACK

Camada por camada — tecnologia, função, e justificativa de escolha.

I TEST AGENTS 02

Playwright — Node.js + Chromium
H2+H3 com TLS handshake real e instrumentável.

k6 — Go runtime
Load test high-throughput; runtime compilado, JS-script.

II PERSONAS 04

Caddy 2.8.x — Go
TLS origin H2+H3, autoTLS, ECDHE+AEAD apenas.

Saleor + Ghost — Django + Node
Real-app backends para testes de App-ID em NGFWs.

mock/har-engine — Go
Custom — controle total dos payloads, baixo footprint.

cert-manager — K8s controller
PKI emitindo certs com IP SANs por VLAN.

III TEST INFRASTRUCTURE 03

FRR (FRRouting) — C container
BGP IETF-padrão, dual-stack v4+v6, suporta 1M+ routes.

VyOS — Debian-based
VPN router open-source — IPsec strongSwan + WireGuard.

iperf3 — C
TCP/UDP throughput padrão da indústria, RFC 6349.

IV ORCHESTRATION & NETWORKING 04

K3s / RKE2 — K8s LTS
Leve, low-overhead, built-in ingress/storage, airgap.

Multus + macvlan — CNI plugin
Multi-NIC K8s; bypassa iptables nas data planes.

NetworkAttachmentDef — CRD
Declarativo de redes secundárias por VLAN.

Cisco Nexus 9000 — Hardware (opc.)
L2 fabric quando l2_fabric=nexus.

V STORAGE & DATABASE 04

PostgreSQL 16+ — OLTP DB
TimescaleDB-friendly; pgvector ready para AI/ML.

PgBouncer — Connection pool
Reduz overhead de conexão; essencial em scale.

MinIO — S3-compatible
Backup target local, airgap-friendly.

Velero+WAL-G+Restic — Backup tools
K8s + PostgreSQL PITR + file-level (ADR 0017).

VI OBSERVABILITY 04

Prometheus — TSDB
Padrão K8s; PromQL expressivo; SLA scrape □ 15s.

Grafana — Dashboarding
Provisionável via JSON/YAML; alerting integrado.

Loki + Promtail — LogQL
Mesma stack Grafana; cost-effective vs Elastic.

snmp_exporter — Prometheus exporter
Lê NGFW/switches via SNMP v2c/v3.

VII DASHBOARD & UI 06

Next.js 15 + React 19 — TypeScript
App Router, RSC, ecossistema maduro.

Drizzle ORM — TS-native
Type-safe queries; migrations SQL-first.

Tailwind CSS — Utility-first
Brand tokens, dark mode nativo.

cmdk + react-flow — UI primitives
Cmd+K palette + drag-and-drop diagrams.

Zod — Schema
Runtime + compile-time; mesma source p/ API+DB.

i18n pt/en/es — Parity test
Mercado-alvo BR/LATAM first-class.

VIII SUPPLY CHAIN & CI/CD 06

Sigstore / cosign — Keyless OIDC
Image signing sem chave a guardar.

Syft — SPDX SBOM
SBOM por release; cosign attestation.

Trivy — Vuln scanner
CVE + secrets + misconfig em containers.

CodeQL — SAST
Análise estática integrada ao GitHub Security.

gitleaks — Secret scan
Pre-commit + CI; histórico completo.

GitHub Actions — CI/CD
Multi-arch QEMU+buildx; auto-merge gated.