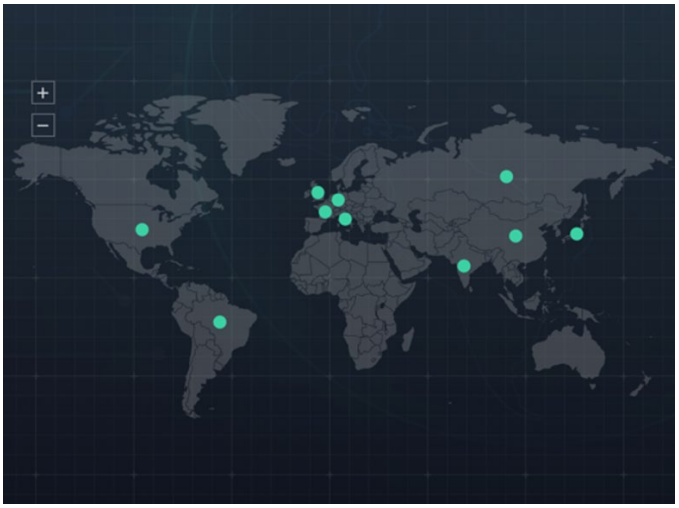
ARA SYSTEM

CONNECTION MANAGEMENT SOFTWARE (PAL-CMS) DATASHEET



The PALAMYS system (Controlled/Customizable Strategic DDoS) is a purpose-built DDoS simulation and penetration-testing platform designed for special units and cyber-range operators who need the most realistic, operationally relevant attack emulation. Developed from real-world cyber-warfare observations and modern DDoS trends, PALAMYS combines powerful, field-proven attack techniques with an operator-friendly control surface so teams can design, schedule, execute and analyze realistic denial-of-service scenarios without excessive operational overhead.

PALAMYS replicates modern adversary behavior across volumetric, protocol and application layers while giving defenders the observability and repeatability required for high-value training and readiness exercises. The system was architected to reflect cyber threat evolution — from amplified reflection attacks and IoT/VM-based botnets to sophisticated HTTP/2 and browser-emulation application floods — and to let blue teams test detection, mitigation and incident-response playbooks under controlled but realistic pressure.

Key capabilities:

- High-impact volumetric & reflection attacks: generate amplified/reflective traffic against web apps, DNS, NTP, COAP, WSD and other vulnerable services to emulate real amplification campaigns.
- Autonomous discovery & augmentation: continuously scan the Internet to discover additional reflector/attack nodes and automatically incorporate them into campaigns.
- Botnet lifecycle management: add, remove and orchestrate attack nodes (bot/VM/reflector fleets) with fine-grained control over behavior, persistence and geographic distribution.
- Scheduled, automated campaigns: create reusable scenarios and run full attack playbooks on demand or on a calendar to support exercises and long-term readiness validation.
- Target reconnaissance & adaptive strategy: automated target profiling (application fingerprinting, API discovery, CDN/WAF detection, origin IP tracing) and automated selection of the most effective attack vectors.
- Visual attack path mapping: interactive visualizations of attack flows, vectors and impact metrics so operators can explain lessons learned to technical and non-technical stakeholders.

Connection Management Software (PAL-CMS)

Introduction

The Connector Management Service is the runtime component that maintains and supervises all active links between the Controller and the distributed attack assets (VM-based bots). It guarantees that bot instances remain responsive and ready to receive operational directives, provides continuous health visibility, and enforces safe, auditable connection handling suitable for controlled cyber-range operations.

Core connection-management features

- **Persistent connection management**

Manage persistent connections with all managed bot endpoints so nodes remain in a ready (standby) state and can accept commands immediately when an operation is triggered.

- **Periodic health & protocol checks**

Automated, scheduled probes to verify bot reachability and responsiveness over commonly abused/IoT protocols: DNS, SSDP, NTP, COAP (Constrained Application Protocol - IoT), WSD (Web Services Dynamic Discovery), and HTTP. Results are logged and surfaced in the Controller dashboard.

- **VM-based bot resource monitoring**

Periodic resource monitoring for emulated bot instances (VM-Base BOTs), including instance count, allocated RAM, CPU usage and observed network throughput to ensure accurate capacity estimates and prevent resource exhaustion.

- **Minimum update frequency**

The connection management software performs a full connection-state refresh and health-check sweep at least once per quarter (≥ 1 time / quarter).

- **Connection lifecycle management**

Add, quarantine, remove or re-provision bot endpoints through the management UI or API with transactional operations and an auditable change log.

- **Automatic reconnection and failover handling**

Built-in logic to attempt safe reconnection for transiently disconnected nodes and to reassign tasks/threads away from unreachable endpoints while preserving campaign integrity.

- **Security & access controls**

Encrypted control channels (TLS), mutual authentication options, and role-checked operations to ensure only authorized roles may modify connection states or issue wide-impact commands.

- **Logging & telemetry**

Detailed event logs for connection checks, status transitions, and administrative operations; telemetry exported to the central Controller for visualization and long-term archiving.

- **APIs & integrations**

RESTful and programmatic interfaces for inventory updates, health query, and bulk operations; supports integration with threat-intel feeds and orchestration tools.

- **Safety & governance mechanisms**

Rate-limiting, maintenance windows, and policy constraints to prevent uncontrolled scanning or excessive probe intensity that could cause collateral impact.

Operational policies & defaults

- **Health-check interval (default)**: configurable; baseline set to weekly for active nodes, quarterly for full-sweep updates (meets the ≥1/quarter requirement).
- **Probe scope**: network reachability, protocol handshake, simple application-layer interaction (where appropriate) and basic resource sampling for VM-Base BOTs.
- **Retention of check results**: historical status snapshots retained per system policy to support audits and trend analysis.

Table 1: Licensing & deployment terms

Item	Specification
Software license	Perpetual or year-base.
Installation license	Unlimited/limited device/server installations permitted under the license terms
Update & maintenance	Maintenance service for updates, security patches and technical support