ARA SYSTEM

CYBER SPACE DENIAL SERVICE DATASHEET

ARA SYSTEM GROUP FZE

Add: Saif Office Q1-07-010/C, Sharjah, United Arab Emirates

Email: sales@ara-system.com

Anonymous Server Service

Introduction

The Anonymous Server Service provides a hardened, privacy-preserving communication layer and It is designed to safeguard control traffic and telemetry between the Controller, connector nodes, and cloud-hosted servers while enabling optional anonymity for sensitive operations. The service combines strong encryption, region-to-region secure tunnels, and support for anonymizing networks to reduce attribution risk and protect operational confidentiality during controlled exercises.

Table 1: Anonymous Server Service Specifications

Component	Minimum specification
CPU	≥ 8 cores
CPU clock speed	≥ 2.0 GHz
RAM	≥ 16 GB
Storage	≥ 256 GB (enterprise SSD/NVMe recommended)
Network	≥ 1 Gbps NIC

Secure communication & anonymity features

- **Encrypted control channels (control servers ↔ cloud servers)**

All management and telemetry links between the Control servers and cloud-resident servers are protected by strong, industry-standard encryption algorithms (e.g., TLS with mutual authentication). End-to-end confidentiality and integrity are enforced to protect command-and-control flows.

- **Inter-region encrypted tunnels**

Encrypted tunnels link server clusters across cloud regions or availability zones so inter-node communications remain confidential and tamper-resistant. Tunnelling supports forward secrecy and secure key rotation to reduce information leak.

- **Integrated anonymizing transport (Tor)**

Native support for Tor allows selected control paths to traverse the Tor network, providing an additional anonymity layer for traffic where reduced attribution is required. Tor integration is configurable at the connector level and can be applied selectively to specific connector pools or operations.

- **Hybrid transport modes**

Operators may choose between low-latency, direct encrypted channels for time-sensitive control and routed anonymized channels for confidentiality-focused tasks. Routing policies and per-operation transport selection are controllable from the management console.

- **Key management & rotation**

Centralized key lifecycle management with automated key rotation, secure storage (HSM support optional), and audited key usage records to meet stringent operational security standards.

- **Authentication & mutual verification**

Mutual host authentication ensures only authorized Controller and connector endpoints establish sessions; certificate-based auth and optional hardware-backed credentials are supported.

- **Traffic minimization & obfuscation**

Optional payload obfuscation and traffic shaping to reduce identifiable patterns in control traffic while maintaining operational reliability.

- **Audit & monitoring**

Encrypted-channel logs (metadata only) and connection health metrics are recorded for audit and troubleshooting without exposing message contents.

Deployment & operational guidance

- **Selective anonymity**: Use Tor-augmented routes only when anonymity is required for a given exercise—default control traffic should use direct, low-latency encrypted channels for performance-sensitive operations.
- **Performance considerations**: Anonymized routes (Tor) introduce additional latency and throughput variability; plan connector placement and task allocation accordingly.
- **Key protection**: Deploy optional HSM or secure vaults for private key storage and ensure strict role separation for key administration.

Database Service

The Database Service is the core data management backbone of the DDoS Simulation System. It securely stores, indexes, and manages all operational data generated by the Controller and Attack Nodes, ensuring integrity, high availability, and fast query performance under heavy workloads. The database infrastructure is engineered for resilience, with redundancy and automated failover mechanisms to sustain mission-critical operations in cyber-range and pentest environments.

Table 2: Database Server Service Specifications

Component	Specification	Description
CPU processing capacity	≥ 8 cores	Multi-core processor optimized for concurrent queries and transaction workloads.
CPU clock speed	≥ 2.0 GHz	Ensures high-speed data access and indexing performance.
RAM	≥ 16 GB	Supports high-throughput caching and parallel query execution.
Storage capacity	≥ 256 GB	Enterprise-grade SSD or NVMe storage ensuring low latency and high IOPS for write-intensive workloads.
Network bandwidth	≥ 1 Gbps	Uplink for synchronization, replication, and rapid data access between Controller and Worker nodes.

Table 3: Data storage and management functions

Function	Description
Centralized botnet and vulnerability management	Stores and tracks the total number and status of all controlled or emulated bots, including :

Function	Description
	-Targets with exploitable vulnerabilities for reflection attacks . - Targets containing exploited vulnerabilities (Backdoor Agents). -Information on simulated bots(VM-Base BOT).
Vulnerability intelligence	Maintains structured records of vulnerable assets discovered through scanning, including service type, exploit vector, and verification state.
Exploit lifecycle data	Records exploited endpoints and backdoor agents currently in use or inactive, supporting lifecycle auditing.
VM-based bot registry	Stores metadata of simulated virtual bots (VM-Base BOTs) including system ID, assigned target, throughput contribution, and operational status.
Attack campaign logs	Preserves historical records of attack plans, execution results, and telemetry data for analysis and reporting.
Security and access control	Enforces role-based access with encrypted connections and authentication inherited from Controller policies.

Table 4: Database architecture model

Design Aspect	Specification / Description
Architecture model	Master–Slave (Primary–Replica) topology for redundancy and scalability.
Replication mode	Synchronous replication between primary and replica databases ensures real-time consistency.
Read scalability	Replica databases (Slave nodes) are optimized for read-only operations to offload traffic from the primary node and enhance system performance.
Automatic failover	When the primary database encounters a fault or downtime, a replica automatically promotes itself to assume the primary role, ensuring continuous availability.
Data integrity	Write-ahead logging (WAL) and journaling mechanisms protect against data loss or corruption during failover.
Backup and recovery	Scheduled automated backups with configurable retention; point-in-time recovery supported.

Server service for connection management software installation

Table 5: Server Service for Connection Management Software

Component	Minimum specification
CPU	≥8 cores
CPU clock speed	≥ 2.0 GHz
RAM	≥ 16 GB
Storage	≥ 256 GB (enterprise SSD/NVMe recommended)
Network	≥ 1 Gbps NIC

Command distribution software installation server service

Table 6: Servver Service for Command Distribution Software

Component	Minimum Specs
CPU	≥ 8 cores
CPU clock speed	≥ 2.0 GHz
RAM	≥ 16 GB
Storage	≥ 256 GB (enterprise SSD/NVMe recommended)
Network	≥ 1 Gbps NIC

Attack Server Services

Table 7: Attack Server Service for Attack Layer

Component	Minimum specification
CPU processing capacity	≥ 8 cores
CPU clock speed	≥ 2.0 GHz
RAM	≥ 16 GB
Storage	≥ 256 GB (enterprise SSD/NVMe recommended)
Network throughput	≥ 10 Gbps NIC

Notes: Attack servers should be deployed on hardened hosts with direct 10 Gbps connectivity to avoid local network bottlenecks. Recommended placement is on provider networks with high egress capacity and predictable routing for realistic traffic shaping.