DEEP PACKET INSPECTION SYSTEM DESIGN DOCUMENT

DeepShield Systems, Inc.

Document Version: 3.2

Last Updated: January 11, 2024

Classification: CONFIDENTIAL

1. INTRODUCTION

1 This Deep Packet Inspection System Design Document ("Design Document") sets forth the proprietary architecture and technical specifications for DeepShield Systems, Inc.'s ("Company") deep packet inspection system ("DPI System") implemented within the DeepShield Maritime Defense Platform(TM).

2 This Design Document and all information contained herein is subject to the Confidentiality and Intellectual Property provisions set forth in Section 8.

2. SYSTEM ARCHITECTURE

1 Core Components

- Packet Capture Engine (PCE-2000)
- Protocol Analysis Module (PAM)
- Threat Detection Core (TDC)
- OT-Specific Pattern Matching Engine
- Real-time Classification System

2 Processing Pipeline

The DPI System implements a multi-stage processing pipeline:

(a) Initial packet capture at wire speed (up to 100Gbps)

(b) Protocol decomposition and state tracking

(c) Deep content inspection

(d) Behavioral analysis

(e) Threat correlation and scoring

3. TECHNICAL SPECIFICATIONS

1 Performance Requirements

- Minimum throughput: 40Gbps per processing unit
- Maximum latency: 100 microseconds
- Packet loss rate: < 0.001%
- Connection tracking capacity: 10M concurrent sessions

2 Protocol Support

The DPI System shall support inspection of:

(a) Industrial protocols including Modbus, DNP3, IEC-61850

(b) Maritime-specific protocols including NMEA 0183/2000

(c) Standard IT protocols (TCP/IP, UDP, ICMP)

(d) Proprietary protocols as defined in Appendix A

4. SECURITY FEATURES

1 Encryption Implementation

- TLS 1.3 support with perfect forward secrecy
- Hardware-based encryption acceleration
- Custom maritime-grade cipher suites
- Quantum-resistant algorithm support (optional module)

2 Access Controls

- Role-based access control (RBAC)
- Multi-factor authentication
- Secure boot process
- Trusted Platform Module (TPM) integration

5. COMPLIANCE AND STANDARDS

1 The DPI System design adheres to:

- IEC 62443 (Industrial Network Security)
- NIST SP 800-82 (Industrial Control Systems)
- Maritime cybersecurity guidelines (IMO MSC-FAL.1/Circ.3)
- GDPR and CCPA requirements where applicable

2 Certification Requirements

All system components must maintain current certifications as listed in Appendix B.

6. INTELLECTUAL PROPERTY PROTECTION

1 Proprietary Elements

The following components constitute protected intellectual property:

(a) Pattern matching algorithms

(b) Threat detection heuristics

(c) Protocol analysis methods

(d) System architecture specifications

(e) Custom acceleration techniques

2 Patent Coverage

This design is protected under U.S. Patents 11,234,567 and 11,345,678 and pending applications PCT/US2023/012345 and PCT/US2023/023456.

7. IMPLEMENTATION REQUIREMENTS

1 Hardware Platform

- Minimum CPU: Intel Xeon Gold 6330 or equivalent
- RAM: 256GB ECC DDR4
- Storage: 2TB NVMe in RAID-1
- Network: Dual 100GbE interfaces

2 Software Dependencies

- DeepShield Core Framework v4.2 or higher
- Maritime Defense Module v2.1
- Threat Intelligence Feed Subscription
- Custom protocol parsers as specified

8. CONFIDENTIALITY AND IP PROVISIONS

1 This Design Document contains trade secrets and confidential information of DeepShield Systems, Inc. All rights reserved.

2 No part of this document may be reproduced, distributed, or transmitted in any form without prior written authorization from the Company's Legal Department.

3 Unauthorized disclosure may result in irreparable harm to the Company and may constitute a violation of the recipient's confidentiality obligations.

9. DOCUMENT CONTROL

Approved by:

Dr. Elena Rodriguez

Chief Security Architect

DeepShield Systems, Inc.

James Morrison

VP of Engineering

DeepShield Systems, Inc.

Date: _

Document Control Number: DPI-DD-2024-001

Classification: CONFIDENTIAL

Distribution: Authorized Personnel Only