SCOPE OF WORK (SOW) FOR NEXT-GENERATION FIREWALL REPLACEMENT AND SECURITY PLATFORM MODERNIZATION

RFP 26-006

Table of Contents

Executive Summary

This Scope of Work (SOW) outlines the comprehensive replacement of 8 end-of-life Cisco ASA 5525 firewalls with modern Next-Generation Firewall (NGFW) solutions and the modernization of the security management platform. The project aims to achieve a minimum 40% improvement in inspection throughput, implement Zero Trust Network Access (ZTNA) capabilities, enhance cloud security integration, and provide advanced threat protection with AI/ML-driven security analytics.

1. Project Overview and Business Drivers

1.1 Current State Challenges

- End-of-life Cisco ASA 5525 firewalls lacking modern security capabilities
- Insufficient throughput for projected network demands
- Limited visibility into encrypted traffic and advanced persistent threats
- Inadequate support for hybrid cloud and remote workforce security
- Reactive security posture without predictive threat intelligence

1.2 Project Objectives

- **Performance Enhancement**: Achieve a minimum 40% increase in firewall inspection throughput
- **Security Modernization**: Implement NGFW with advanced threat protection, ZTNA, and SASE capabilities
- **Cloud Integration**: Enable seamless hybrid and multi-cloud security management
- **AI/ML Integration**: Deploy machine learning-based threat detection and automated response
- **Compliance Readiness**: Ensure compliance with current and emerging regulatory requirements
- **Future-Proofing**: Select solutions with a minimum 7-year lifecycle and regular feature updates

2. Technical Requirements and Specifications

2.1 Performance Requirements

- **Minimum Throughput**: 40% improvement over current ASA 5525 performance
- **Inspection Capabilities**: Full SSL/TLS inspection without performance degradation
- **Concurrent Sessions**: Support for a minimum of 1,000,000 concurrent sessions per device
- **VPN Capacity**: Support for 1,000+ concurrent SSL VPN users per device
- **Latency**: Maximum 10ms additional latency for inspected traffic

2.2 Security Feature Requirements

- **Next-Generation Features**:
    - Application visibility and control
    - User identity-based policies
    - Advanced threat prevention (ATP)
    - Behavioral analytics and anomaly detection
    - DNS security and DGA detection
    - IoT device identification and segmentation
- **Zero Trust Capabilities**:
    - Micro-segmentation
    - Identity-based access control
    - Continuous verification and monitoring
    - Least privilege access enforcement
- **Cloud Security Integration**:
    - SASE (Secure Access Service Edge) compatibility
    - Cloud-native security policy management
    - Multi-cloud visibility and control
    - Container and serverless security integration

2.3 Required Firewall Solutions

Cisco Next-Generation Solutions

Primary Recommendation: Cisco Firepower 3100 Series

- **Cisco FPR-3105**: Up to 10 Gbps firewall throughput, 3.2 Gbps TLS
- **Cisco FPR-3110**: Up to 17 Gbps firewall throughput, 4.8 Gbps threat defense
- **Management**: Cisco Secure Firewall (Firepower Management Center-FMC 7.4+)
- **Licensing**: Threat Defense licenses, Advanced Malware Protection (AMP)
- **Support Lifecycle**: Minimum 7 years with regular software updates

3. Detailed Scope of Work

3.1 Discovery and Assessment Phase

- **Network Architecture Analysis**:
    - Traffic pattern analysis and bandwidth utilization assessment
    - Application discovery and classification
    - Security policy audit and optimization opportunities
    - Cloud connectivity and hybrid architecture evaluation
- **Performance Baseline**:
    - Current throughput measurements and bottleneck identification
    - Latency analysis and quality of service requirements
    - Capacity planning for 3-year growth projection
- **Security Gap Analysis**:
    - Threat landscape assessment specific to the organization's industry
    - Compliance requirement mapping (PCI-DSS, HIPAA, etc.)
    - Current security tool integration assessment

3.2 Solution Design and Architecture

- **High-Level Design (HLD)**:
    - Network topology and traffic flow optimization

    - High availability and disaster recovery design
    - Integration with existing security infrastructure
- **Detailed Technical Design**:
    - Interface configuration and VLAN assignments
    - Routing protocols and network segmentation strategy
    - VPN architecture (IPSec, SSL VPN, ZTNA)
    - Management and monitoring integration

3.3 Procurement and Licensing

- **Hardware/Virtual Appliances**:
    - Firewall devices with appropriate performance specifications
    - High availability pairs where required
    - Necessary accessories and support contracts
- **Software Licensing**:
    - Threat prevention and advanced security subscriptions
    - Management platform licensing
    - Cloud security service subscriptions
    - Professional services and training credits

3.4 Implementation and Migration

- **Pre-Deployment Configuration**:
    - Device staging and initial configuration in a controlled environment
    - Policy migration and optimization
    - Integration testing with management platforms
    - Integration with existing Cisco Tools in the environment

- **Phased Deployment**:
    - Pilot deployment with non-critical traffic
    - Gradual migration with rollback procedures

    - Production cutover with minimal downtime windows
- **Post-Deployment Optimization**:
    - Performance tuning and policy refinement
    - Security efficacy validation
    - Integration with workflows

3.5 Testing and Validation

- **Functional Testing**:
    - Traffic flow and application performance validation
    - Security policy enforcement verification
    - VPN and remote access functionality testing
- **Security Testing**:
    - Penetration testing and vulnerability assessment
    - Threat simulation and response validation
    - Compliance audit and certification support
- **Performance Testing**:
    - Throughput and latency benchmarking
    - Concurrent session and VPN user testing
    - Failover and recovery time validation

4. Project Timeline and Milestones

S/N	Phase	Duration	Key Deliverables
1	Discovery & Assessment	1 weeks	Current state assessment, gap analysis, performance baseline
2	Solution Design	2 weeks	HLD, detailed design, procurement specifications
3	Procurement	3-4 weeks	Hardware/software delivery, licensing activation
4	Configuration & Testing	2 weeks	Staged configuration, policy migration, integration testing
5	Pilot Deployment	1 week	Limited production deployment, validation

6	Production Migration	1-2 weeks	Phased cutover, optimization, monitoring
7	Testing & Validation	1 week	Security testing, performance validation, compliance verification
8	Knowledge Transfer	1 week	Training, documentation, operational handover
9	Hypercare Support	4 weeks	24/7 support, optimization, issue resolution

Total Project Duration: 11 -12 weeks

5. Deliverables and Success Criteria

5.1 Technical Deliverables

1. **Comprehensive Assessment Report** with current state analysis and recommendations
2. **Solution Architecture Documentation,** including HLD and detailed technical designs
3. **Migration Runbooks** with step-by-step procedures and rollback plans
4. **Configured NGFW Infrastructure** meeting all performance and security requirements
5. **Integrated Management Platform** with centralized policy management
6. **Security Policy Framework** optimized for Zero Trust principles
7. **Performance Validation Report** demonstrating 40%+ throughput improvement
8. **Security Testing Results,** including penetration test and vulnerability assessment reports
9. **Operational Documentation,** including troubleshooting guides and maintenance procedures
10. **Recommend Training Materials** and knowledge transfer sessions for security team
11. Five-Year Operational Cost Breakdown
12. Optional Managed Services Proposal

5.2 Success Criteria

- **Performance**: Minimum 40% improvement in firewall inspection throughput
- **Availability**: 99.9% uptime during steady state operations
- **Security**: Zero critical vulnerabilities and 100% policy compliance
- **Migration**: Successful cutover with less than 4 hours total downtime per location
- **User Experience**: No degradation in application performance or user connectivity
- **Knowledge Transfer**: IT team capable of day-to-day operations and Level 1 troubleshooting

6. Risk Management and Mitigation

6.1 Technical Risks

- **Performance Issues**: Comprehensive testing and gradual migration approach
- **Compatibility Problems**: Thorough integration testing with existing infrastructure
- **Security Gaps**: Parallel operation during transition with comprehensive monitoring

6.2 Business Risks

- **Extended Downtime**: Detailed rollback procedures and 24/7 support during migration
- **Budget Overruns**: Fixed-price engagement with change control procedures
- **Timeline Delays**: Buffer time in project schedule and alternative deployment scenarios
- **SLA for Critical Outages**: SLA of 1–2 hours for critical outages

7. Ongoing Support and Maintenance

7.1 Hypercare Period (60 days)

- 24/7 monitoring and support
- Performance optimization and tuning

- Issue escalation and resolution
- Weekly health check reports

7.2 Long-term Support Strategy

- Quarterly security policy reviews and updates
- Annual security assessments and optimization
- Firmware and software update management
- Capacity planning and lifecycle management
- Optional Managed Services: Vendor to provide a proposal for managed services, including scope, SLAs, and pricing for long-term outsourced support and monitoring

8. Investment Summary and ROI

8.1 Key Investment Areas

- Next-generation firewall hardware/software
- Advanced security subscriptions and licensing
- Professional services and implementation
- Training and knowledge transfer
- Ongoing support and maintenance

8.2 Expected Return on Investment

- **Security**: Reduced risk exposure and faster threat response
- **Performance**: Improved application performance and user productivity
- **Operational**: Reduced management overhead and automated policy enforcement
- **Compliance**: Simplified audit processes and regulatory adherence
- **Future-Proofing**: Platform ready for emerging security requirements

9. Vendor Qualification and Selection Criteria

9.1 Mandatory Requirements

- Minimum 7-year product lifecycle commitment
- 24/7 technical support with 4-hour response time
- Local presence and certified implementation partners
- SLA for Critical Outages: 1–2 hour response time
- Regular threat intelligence updates and signature delivery
- Compliance with relevant industry standards and certifications
- Dedicated Account Representative assigned.

9.2 Preferred Qualifications

- Cloud-native management capabilities
- AI/ML-based threat detection and response
- Integration with major cloud platforms (AWS, Azure, OCI)
- API-driven automation and orchestration capabilities
- Strong third-party security ecosystem integration

10. LBT Locations

Firewalls will be installed in all of these locations:

- LBT1 – 1963 E. Anaheim St. Long Beach, CA 90813.
- LBT2 – 6860 Cherry Ave. Long Beach, CA 90805.
- LBTCO – 4801 Airport Plaza Dr. Long Beach, CA 90808.