## Strategic Advisory: ICS/OT Segmentation Build vs. Buy Decision

### Executive Summary

The transition from traditional on-premises firewalls to cloud-based virtual firewalls for north/south traffic creates a critical opportunity to reimagine east/west traffic security in WWOps ICS/OT environment. Based on CLS’ analysis, **an iterative build approach using lightweight Linux-based segmentation** aligns optimally with Amazon's innovation culture while addressing core security requirements. This approach offers:

* **Dramatically lower capital expenditure** with baseline models at $200-$300 per unit and advanced models at $1,500 per unit, resulting in potential savings of $25-45 million across 15,000 units
* **Faster deployment** of essential security controls with significantly lower initial investment
* **Tailored protection** specific to WWOps ICS/OT environment without extraneous features
* **Cultural alignment** with Amazon's history of innovation and disruption
* **Evolutionary adaptability** to incorporate new requirements as they emerge
* **No recurring annual licensing costs** that would create budgetary uncertainty

CLS recommends a phased implementation starting with a minimum viable secure solution focused on traffic filtering, address translation, state tracking, service management (DNS/NTP redirection), FQDN based traffic filtering, High Availability through rapid recovery, traffic flow metrics, and logging. This feature set, minus FQDN based filtering, aligns to the incumbent services available in the current common firewalls. This foundation can be iteratively enhanced based on measured requirements rather than speculative needs. To ensure team alignment, we propose a collaborative lab environment where both approaches can be tested against real-world scenarios using a clear evaluation framework.

### Build vs. Buy Analysis for ICS/OT Environments

#### Technical Considerations

|  |  |  |
| --- | --- | --- |
| **Factor** | **Custom Build Approach** | **Commercial Industrial Firewalls** |
| **Protocol Support** | Initially limited to essential ICS protocols (Modbus, DNP3, etc.) with capability to add others as needed | Comprehensive pre-built support for numerous protocols, many likely unused |
| **Deployment Timeline** | Faster initial deployment (8-12 weeks for MVP) | Longer procurement and implementation cycle (6-9 months) |
| **Performance** | Optimized for specific traffic patterns in WWOps environment | Generic optimization that may include overhead for unused features |
| **Scalability** | Vertically scalable through high capacity hosts | Typically requires additional licenses or hardware |
| **Integration** | Designed specifically for Amazon’s ecosystem | May require adapters or middleware for full integration |
| **Customization** | Complete control over features and behaviors | Limited to vendor's configuration options |
| **Maintenance** | Requires internal expertise and ownership | Vendor-managed updates and patches |

#### Financial Analysis

The financial impact of this decision is substantial given the 15,000 unit deployment scale:

|  |  |  |
| --- | --- | --- |
| **Cost Category** | **Custom Build Approach** | **Commercial Industrial Firewalls** |
| **Hardware Costs (Baseline)** | $3-4.5 million ($200-300 × 15,000) | $30 million ($2,000 × 15,000) |
| **Hardware Costs (Advanced)** | $22.5 million ($1,500 × 15,000) | $52.5-67.5 million ($3,500-4,500 × 15,000) |
| **Development Costs** | $1.5-2.5 million (team of 8-10 developers for 12 months) | Minimal customization costs |
| **Annual Licensing** | None | Undetermined but likely 15-25% of hardware costs annually |
| **Maintenance Costs** | $800,000-1.2 million annually (team of 5-8 engineers) | Support contracts plus internal resources |
| **5-Year TCO (Baseline)** | $8-12 million | $52.5-67.5 million (including estimated licensing) |
| **Cost Savings** | $40-55.5 million over 5 years | Baseline for comparison |

Even allocating substantial resources for development and maintenance, the build approach represents a potential savings of $40-55.5 million over a 5-year period. This financial difference is significant enough to overcome many of the technical advantages of commercial solutions.

#### Cultural and Strategic Alignment

Amazon's history of innovation and disruption is a crucial competitive advantage. The custom build approach reinforces this culture by:

* **Fostering innovation competency** among security team members
* **Developing institutional knowledge** specific to WWOps OT environment
* **Creating opportunities for cross-functional collaboration** between security, operations, and development teams
* **Demonstrating commitment to Amazon's innovative ethos**
* **Establishing security as an innovation partner** rather than a constraint

Commercial solutions, while providing immediate feature completeness, may reinforce a consumption mindset rather than a creation mindset. This subtle shift can impact how security is perceived within the organization and influence future decision-making.

### Technical Architecture Recommendation

CLS recommends a **hybrid approach heavily weighted toward the build option** with the following components:

* **Core Segmentation Layer:** Custom-built lightweight Linux-based firewall nodes deployed as container instances for east/west traffic control
* **Central Management Plane:** Simple orchestration system for policy deployment and configuration management
* **Monitoring and Analytics:** Integration with existing SIEM/SOC infrastructure using standard protocols
* **Industrial Protocol Inspection**: Focused parsing and validation for critical ICS protocols in your environment
* **Future Expansion Hooks:** Well-defined APIs and interfaces for adding capabilities as requirements emerge

The architecture employs a distributed enforcement model with centralized policy management, allowing for deployment flexibility across various OT network segments. This approach creates clear boundaries between operational zones while maintaining the performance requirements of industrial systems.

### Phased Implementation Roadmap

#### Phase 1: Minimum Viable Secure Solution (Weeks 1-12)

* Define core traffic filtering requirements through OT network traffic analysis
* Develop and test baseline packet filtering for critical asset protection
* Implement logging and basic alerting infrastructure
* Deploy to pilot zone with side-by-side monitoring (non-blocking)
* **Estimated cost: $1.2-1.5 million** (development + initial 500 baseline units)

#### Phase 2: Enhanced Capabilities (Weeks 13-24)

* Add protocol-specific inspection for primary ICS protocols
* Develop custom rules based on observed traffic patterns
* Implement automated response to common threat scenarios
* Expand deployment to additional zones in blocking mode
* **Estimated cost: $2.9-3.5 million** (continued development + 2,500 additional baseline units)

#### Phase 3: Optimization and Scale (Weeks 25-36)

* Performance tuning based on production metrics
* Automation of routine management tasks
* Development of custom dashboards for OT security visibility
* Full production deployment with continuous improvement cycle
* **Estimated cost: $3.5-4.8 million** (7,000 additional baseline units)

#### Phase 4: Advanced Features (Weeks 37+)

* Integration with threat intelligence feeds
* Development of anomaly detection capabilities
* Implementation of advanced behavioral analytics
* Capacity expansion based on actual utilization metrics
* **Estimated cost: $2.5-3.5 million** (5,000 advanced units for critical zones)

### Risk Assessment and Mitigation

#### Build Approach Risks

|  |  |
| --- | --- |
| **Risk** | **Mitigation Strategy** |
| **Inadequate Feature Development** | Start with critical protections and use agile development methods to rapidly address gaps; allocate $500,000 contingency budget for additional developers if needed |
| **Team Knowledge Gaps** | Partner with Linux security specialists for initial development ($150,000-250,000 consulting budget); implement knowledge transfer program |
| **Development Delays** | Use time-boxed sprints with clear priorities; maintain option to deploy commercial solution in critical areas if necessary (budget for 500 commercial units as contingency) |
| **Maintenance Burden** | Design for maintainability with thorough documentation; automate routine maintenance tasks; budget for appropriate maintenance team (5-8 dedicated engineers) |
| **Staffing Changes** | Cross-train multiple team members; document extensively; use standard development practices; implement retention incentives for key personnel |

#### Buy Approach Risks

|  |  |
| --- | --- |
| **Risk** | **Mitigation Strategy** |
| **Excessive Complexity** | Rigorous feature evaluation to enable only necessary capabilities |
| **Vendor Lock-in** | Negotiate favorable contract terms; develop exit strategy |
| **Compatibility Issues** | Extensive pre-purchase testing in lab environment |
| **Cost Escalation** | Careful TCO analysis including hidden costs; fixed-price agreements |
| **Cultural Misalignment** | Internal messaging emphasizing strategic vendor partnerships |
| **Budget Overruns** | The $40-55.5 million cost difference creates significant financial risk with limited mitigation options |

### Team Alignment Recommendations

The current team dynamic reflects a common pattern when transitioning from traditional security models to more innovative approaches. We recommend:

* **Financial Transparency Workshop**: Present detailed TCO analysis showing the dramatic cost difference between approaches
* **Joint Design Workshop**: Conduct a facilitated 2-day session where both approaches are mapped against actual requirements
* **Proof of Concept Competition**: Create small teams to demonstrate both approaches in a lab environment
* **Shared Evaluation Framework**: Develop objective criteria collaboratively that both solutions must meet
* **Skills Investment Program**: Create learning paths for team members to develop skills needed for the build approach
* **Recognition Structure**: Implement rewards for innovation and creative problem-solving
* **Clear Decision Authority**: Establish transparent process for resolving technical disagreements

### Compromise Solution Elements

While CLS recommends primarily pursuing the build approach, incorporating these elements of commercial solutions may address team concerns:

* **Selective Commercial Deployment**: Deploy commercial firewalls in 1-2 most critical zones (300-500 units) while building custom solution for others
* **Commercial Management Console**: Consider using a commercial management platform that can also integrate custom enforcement points
* **Vendor Advisory Relationship**: Maintain relationship with preferred vendor for consultation without full product deployment
* **Escape Hatch Planning**: Develop clear criteria that would trigger pivoting to commercial solution if build approach falters

### Success Metrics and Evaluation Framework

#### Key Performance Indicators

* **Security Effectiveness**: Percentage of unauthorized connection attempts blocked
* **Deployment Velocity**: Time to secure new OT network segments
* **Operational Impact**: Number of legitimate operations blocked or delayed
* **Resource Utilization**: CPU, memory, and network overhead of security controls
* **Team Capability Growth**: Measured increase in team skills and confidence
* **Innovation Transfer**: Adoption of techniques developed for OT in other areas
* **Financial Efficiency**: Actual costs compared to projections for both capital and operational expenses

#### Feature Addition Triggers

New capabilities should only be added when one of these conditions is met:

* **Demonstrated Threat**: Evidence of specific attack techniques targeting your environment
* **Regulatory Requirement**: New compliance mandates that specifically require the feature
* **Operational Need**: Business process changes requiring new security capabilities
* **Efficiency Opportunity**: Feature would significantly reduce operational overhead

### Conclusion

The build vs. buy decision for ICS/OT segmentation represents more than just a technical choice—it's a statement about CLS’ identity and its relationship to the broader company culture. By embracing an iterative build approach, CLS reinforces the innovative spirit that has defined Amazon while addressing essential security requirements.

With a potential cost difference of $40-55.5 million over five years, the financial case for the build approach is compelling. This difference allows for significant investment in development and maintenance resources while still delivering substantial savings. The absence of recurring licensing costs also provides greater budgetary predictability.

A custom-built solution focusing initially on core protections allows you to deploy critical controls quickly, learn from actual usage patterns, and evolve the solution based on evidence rather than assumptions. This approach aligns technical needs with cultural values while positioning the security team as innovation partners.

The recommended hybrid strategy mitigates key risks while creating space for the security team to develop new capabilities. By establishing clear evaluation criteria and decision points, you maintain flexibility to adjust course if requirements change or challenges emerge.

For an organization with Amazon’s history of innovation and disruption, facing the scale of deployment WWOps requires, this approach represents the optimal balance of security, agility, and financial responsibility.