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

### Executive Summary

The transition from traditional on-premises firewalls to cloud-based virtual firewalls for north/south traffic necessitates a robust, immediately effective solution for securing east/west traffic in your ICS/OT environment. Based on CLS’ comprehensive analysis, **investing in purpose-built commercial industrial firewalls** represents a strategic approach for your organization despite higher upfront costs. This strategy offers:

* **Immediate comprehensive protection** with validated security controls specifically designed for industrial environments
* **Reduced operational risk** through vendor-backed implementation and support
* **Faster time-to-security** with pre-configured capabilities for industrial protocols
* **Efficient resource allocation** allowing your team to focus on strategic integration rather than firewall development
* **Regulatory compliance assurance** with solutions pre-certified for relevant standards

While acknowledging the significant price difference between commercial solutions ($2,000-$4,500 per unit) and custom build options ($200-$1,500 per unit), we propose that the **total cost of ownership must be evaluated beyond hardware costs alone**. The critical nature of ICS/OT environments demands proven, tested solutions with dedicated support ecosystems to ensure continued protection against evolving threats.

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

#### Technical Considerations

|  |  |  |
| --- | --- | --- |
| **Factor** | **Commercial Industrial Firewalls** | **Custom Build Approach** |
| **Protocol Support** | Comprehensive, tested support for industrial protocols with regular updates | Limited to protocols specifically implemented by your team, with uncertain quality |
| **Threat Intelligence** | Continuous vendor updates based on global threat data | Reliant on in-house research or open-source intelligence |
| **Deployment Timeline** | 3-4 months for full enterprise deployment | 12-18 months for equivalent capability development |
| **Performance Assurance** | Vendor-guaranteed performance metrics with supporting hardware | Unpredictable performance requiring extensive testing and tuning |
| **Scalability** | Purpose-built scaling with clear capacity planning | Custom scaling architecture requiring additional development |
| **Certification** | Pre-certified for relevant standards (IEC 62443, NERC CIP) | Custom certification process requiring significant documentation |
| **Support** | | 24/7 vendor support with defined SLAs | Reliant on internal expertise with potential single points of failure |

### Financial Analysis

It's critical to assess the total cost of ownership beyond hardware costs:

|  |  |  |
| --- | --- | --- |
| **Cost Category** | **Commercial Industrial Firewalls** | **Custom Build Approach** |
| **Hardware Costs (Baseline)** | $30 million ($2,000 × 15,000) | $3-4.5 million ($200-300 × 15,000) |
| **Hardware Costs (Advanced)** | $52.5-67.5 million ($3,500-4,500 × 15,000) | $22.5 million ($1,500 × 15,000) |
| **Annual Licensing** | Estimated at 15-25% of hardware costs | None |
| **Implementation Professional Services** | $2-3 million (vendor-provided) | Not applicable |
| **Development Costs** | | Not applicable | $8-12 million (team of 20-30 developers for 18-24 months) |
| **Hidden Development Costs** | Not applicable | $4-6 million (infrastructure, testing, tools, delays) |
| **Ongoing Maintenance & Support** | $4.5-7.5 million annually (licensing + internal resources) | $3-4.5 million annually (larger team of 15-20 engineers) |
| **Security Incident Risk** | Lower (estimated 30-40% reduction in probability) | Higher during early deployment phases |
| **Cost of Security Breach** | Industry average: $2.8-4.2 million per incident | Same baseline, but higher probability |
| **Risk-Adjusted Value (5 years)** | $5.8-8.4 million in avoided breach costs | Baseline for comparison |

While the hardware cost difference is significant, **CLS estimate that the true 5-year TCO difference is closer to $15-25 million** rather than the $40-55 million suggested by hardware costs alone. This accounts for:

* Significantly higher development and maintenance costs for the build option
* Higher security risk during development and early deployment
* Productivity losses associated with custom development
* Additional staffing needs for a custom solution

### Risk Management Considerations

ICS/OT environments present unique security challenges that commercial solutions are specifically designed to address:

* **Protocol Vulnerabilities**: Industrial protocols often lack built-in security features; commercial solutions offer specialized inspection and protection capabilities
* **Critical Impact**: Breaches in OT environments can have physical safety implications, demanding proven protection measures
* **Regulatory Compliance**: Industrial environments face specialized compliance requirements that commercial solutions are pre-configured to address
* **Operational Stability**: Commercial solutions undergo extensive testing to ensure they don't disrupt critical industrial processes
* **Unique Attack Vectors**: ICS-specific attack techniques require specialized detection technologies developed by industrial security experts

### Technical Architecture Recommendation

CLS recommends a **phased commercial ICS/OT firewall deployment** with the following approach:

* **Targeted Commercial Deployment**: Deploy specialized OT security appliances at the most critical 30% of network boundaries first
* **Centralized Management Console**: Implement vendor-provided unified management platform for policy orchestration
* **Industrial Protocol Deep Inspection**: Utilize vendor-developed protocol parsers for all relevant industrial protocols
* **Integration Layer**: Develop custom integration components to connect commercial solution with existing security infrastructure
* **Security Monitoring**: Leverage vendor-provided visibility tools with custom dashboards for your specific environment

This architecture provides defense-in-depth specifically designed for industrial systems while allowing your team to focus innovation efforts on integration and operational workflows rather than core security functions.

### Financial Optimization Strategy

To address the significant cost concerns:

* **Vendor Negotiation Strategy**:
  + Multi-year enterprise agreement to secure 25-40% discount off list pricing
  + Volume-tiered pricing structure with escalating discounts
  + Cap on annual maintenance increases (maximum 3% annually)
  + No-cost proof-of-concept for initial deployment zone
* **Phased Deployment to Optimize Expenditure**:
  + Year 1: Deploy to most critical 30% of zones (4,500 units)
  + Year 2: Expand to next 30% of zones (4,500 units)
  + Year 3: Complete deployment to remaining 40% (6,000 units)
* **Total Cost Optimization**:
  + Eliminate redundant security tools that overlap with commercial capabilities
  + Leverage vendor professional services credits
  + Consolidate management consoles where possible
  + Negotiate training and certification costs into purchase agreement

With these strategies, we believe the hardware cost could be reduced by 30-35%, narrowing the financial gap between build and buy approaches.

### Phased Implementation Roadmap

#### Phase 1: Assessment and Selection (Weeks 1-6)

* Conduct detailed requirements gathering and industrial network traffic analysis
* Evaluate vendor solutions against operational requirements
* Perform proof-of-concept testing in lab environment
* Select optimal commercial platform based on performance and capability metrics
* **Estimated cost: $250,000-400,000** (professional services and internal resources)

#### Phase 2: Initial Critical Deployment (Weeks 7-16)

* Implement commercial solution at 30% most critical boundaries (4,500 units)
* Develop and tune rulesets based on observed traffic patterns
* Train operations and security teams on management platform
* Establish baseline metrics for normal operations
* **Estimated cost: $9-10.8 million** (hardware + implementation services)

#### Phase 3: Expansion and Integration (Months 5-12)

* Gradually transition from monitoring to enforcement mode
* Deploy to next 30% of industrial zones (4,500 additional units)
* Integrate with existing security monitoring infrastructure
* Implement automated response workflows for common scenarios
* **Estimated cost: $9-10.8 million** (hardware + implementation services)

#### Phase 4: Full Deployment and Innovation (Year 2)

* Complete deployment to remaining 40% of zones (6,000 units)
* Develop custom integrations with business systems
* Create automated workflows for change management
* Implement advanced analytics using firewall telemetry
* **Estimated cost: $12-14.4 million** (hardware + implementation services)

### Risk Assessment and Mitigation

#### Buy Approach Risks

|  |  |
| --- | --- |
| **Risk** | **Mitigation Strategy** |
| **Significant Capital Expenditure** | Phased deployment approach; negotiate enterprise pricing with long-term agreement |
| **Vendor Lock-in** | Implement standards-based interfaces; maintain multi-vendor strategy |
| **Annual Licensing Costs** | Negotiate price protection; cap annual increases; secure enterprise license agreement |
| **Feature Bloat** | Implement strict change control; disable unnecessary capabilities |
| **Poor Vendor Support** | Establish clear SLAs with penalties; maintain secondary vendor relationships |
| **Cultural Resistance** | Focus innovation on how the solution is implemented and integrated |

#### Build Approach Risks

|  |  |
| --- | --- |
| **Risk** | **Mitigation Strategy** |
| **Development Failures** | Significant risk of incomplete or inadequate security controls |
| **Knowledge Concentration** | Dependency on few individuals with specialized knowledge |
| **Delayed Protection** | Extended vulnerability window during development |
| **Inconsistent Coverage** | Uneven protection across different protocols and attack vectors |
| **Maintenance Burden** | Ongoing diversion of resources from strategic initiatives |
| **Hidden Costs** | Development costs typically exceed projections by 50-200% |

### Innovative Implementation Approach

While recommending commercial solutions, we emphasize channeling your innovation culture into how these solutions are deployed and operationalized:

* **Custom Orchestration Layer:** Develop innovative deployment and configuration automation
* **Advanced Analytics**: Build custom intelligence using data from commercial platforms
* **Integration Innovation**: Create novel connections between OT security and business processes
* **Operational Playbooks**: Develop industry-leading response procedures leveraging vendor capabilities
* **Cross-Domain Visibility**: Pioneer new approaches to unifying IT/OT security monitoring

This approach allows your team to focus innovation where it adds the most value, while leveraging vendor expertise for core security functions.

## Cost-Sensitive Compromise Solution

Given the significant cost concerns, we suggest this hybrid approach:

* **Tiered Security Model**:
  + Deploy commercial firewalls to most critical zones (30% of deployment, 4,500 units)
  + Develop simplified custom solution for lower-risk areas (70% of deployment, 10,500 units)
  + Utilize unified management platform across both deployment types
* **Cost Structure**:
  + Critical Zones: $9-10.8 million (commercial solution)
  + Lower-Risk Zones: $2.1-3.15 million (custom solution at $200-300 per unit)
  + Management Platform: $1.5-2 million (commercial platform with integration)
  + Custom Development: $3-4 million (simplified custom solution)
  + \*\*Total: $15.6-19.95 million\*\* (vs. $30-67.5 million for full commercial deployment)
* **Implementation Approach**:
  + Begin commercial deployment immediately for critical zones
  + Develop simplified custom solution in parallel for lower-risk zones
  + Create integration layer between commercial and custom solutions
  + Unified policy management across both platforms

This compromise approach reduces the capital expenditure by 45-65% while still providing enterprise-grade protection for critical assets.

### Team Alignment Recommendations

To address the current team dynamic and leadership preferences:

* **Threat-Based Assessment Workshop**: Evaluate security requirements based on actual threats rather than theoretical maximums
* **Cost-Benefit Analysis Session**: Present transparent TCO analysis including development and maintenance costs
* **Phased Deployment Planning**: Develop detailed implementation plan that addresses both security priorities and budget constraints
* **Innovation Focus Groups**: Identify areas where custom development adds the most value within a commercial framework
* **Vendor Collaboration Lab**: Create dedicated environment for testing commercial solutions against specific requirements
* **Skills Development Program**: Establish learning paths for team members to become elite implementers of industrial security technologies

### Success Metrics and Evaluation Framework

#### Key Performance Indicators

* **Security Coverage**: Percentage of industrial protocols and assets protected
* **Deployment Efficiency**: Cost per protected zone compared to industry benchmarks
* **Time to Detection**: Average time to identify potential security incidents
* **Time to Protection**: Speed of deploying new protections against emerging threats
* **Operational Stability**: Measurement of system availability and performance
* **Team Efficiency**: Resource hours dedicated to maintenance vs. strategic initiatives
* **Financial Efficiency**: Actual costs compared to budgeted amounts across all phases

#### Ongoing Assessment Framework

Establish a quarterly review process to evaluate:

* **Effectiveness**: Protection capability against known and emerging threats
* **Operational Impact**: Minimal interference with legitimate industrial operations
* **Management Efficiency**: Time required for policy changes and updates
* **Support Quality**: Vendor responsiveness and resolution rates
* **TCO Analysis**: Regular reassessment of total cost against value delivered
* **Innovation Opportunities**: Areas where custom development would add significant value

### Conclusion

While the hardware cost difference between commercial and custom-built solutions is substantial, the security of industrial control systems represents a domain where proven, purpose-built commercial solutions offer compelling advantages for your most critical assets.

The compromise approach we've outlined—deploying commercial solutions to critical zones while developing simplified custom solutions for lower-risk areas—balances financial constraints with security requirements. This hybrid model represents a potential cost reduction of 45-65% compared to a full commercial deployment while still providing enterprise-grade protection where it matters most.

By redirecting your innovation culture toward implementation, integration, and operational excellence, you can achieve a superior security posture more rapidly while still maintaining your company's innovative edge. This approach balances immediate security needs with long-term strategic goals.

We recommend proceeding with a careful vendor selection process focused on identifying solutions that offer both robust protection and sufficient flexibility to accommodate your specific operational requirements and integration needs. Simultaneously, we suggest establishing a development team focused on creating simplified solutions for lower-risk environments, allowing you to maximize both security effectiveness and cost efficiency.