

# Perimeter Hardening: Palo Alto Firewall + Site-to-Site IPsec VPN

*Case Study — Network Engineer I, Aston Technologies*

---

## OVERVIEW

This project paired two related pieces of security work: building secure site-to-site IPsec connectivity for a new site, and using the review process as an opportunity to tighten an existing firewall rule base that had grown overly permissive over time.

## PROBLEM

Existing Palo Alto and Cisco Firepower policy included broad, “any-any” style rules accumulated over time, and a new site needed secure, encrypted connectivity back to the core network without the cost and lead time of a dedicated circuit.

## PROCESS

- Authored CAB documentation for both the new IPsec tunnel and the associated policy changes
- Defined pre- and post-change validation steps before touching production policy
- Designed a site-to-site IPsec tunnel to carry the new site's traffic securely over existing internet transport
- Reviewed existing rule base against actual observed traffic patterns to identify safe narrowing opportunities

## SOLUTION

Configured and validated the IPsec tunnel end-to-end on the Palo Alto NGFW, then tightened firewall policy in tandem — replacing broad allow rules with scoped rules matched to the traffic patterns identified during review, and applying corresponding updates on Cisco Firepower.

## VERIFICATION

Confirmed tunnel stability under load, correct traffic routing through the new policy set, and no unintended loss of access for legitimate traffic before closing out the change window.

## OUTCOME

Delivered secure site connectivity without new circuit costs, and measurably reduced the number of overly permissive rules as part of an ongoing security hardening initiative — the actual Change Request Form and MOP used are included as a companion document.

## SKILLS DEMONSTRATED

Palo Alto Networks NGFW policy configuration • Cisco Firepower change execution • Site-to-site IPsec VPN design • Security policy review & hardening • Change management (MOP authorship, CAB documentation)