Change Request Form & Method of Procedure

Site-to-Site IPsec VPN & Firewall Policy Hardening

CHANGE REQUEST SUMMARY

Change Request No.: SEC-2026-04

Project: New Site IPsec Connectivity & Firewall Policy Hardening

Requested By: Justin K. Bowden, Network Engineer I

Department: Network Engineering / Security

Change Priority: Medium

Change Impact: Major

Environments Impacted: Palo Alto NGFW perimeter policy; Cisco Firepower policy set; new site connectivity

DESCRIPTION OF CHANGE

Establish a site-to-site IPsec VPN tunnel between a new site and the core network on the Palo Alto NGFW, and review/tighten existing firewall security policy on both Palo Alto and Cisco Firepower as part of an ongoing hardening initiative.

REASON FOR CHANGE

- Provide secure connectivity for a new site without a dedicated WAN circuit
- Reduce the attack surface created by overly broad, legacy firewall rules
- Bring policy in line with current traffic patterns and least-privilege practice

CHANGE IMPACT EVALUATION

Change Type	Impacted
Network	Yes
Security	Yes
Application	Possible — pending rule scoping
Procedures	Yes

RESOURCE REQUIREMENTS

Personnel: 1 Network Engineer, 1 Security reviewer/approver. Hardware/Software: Palo Alto NGFW management access, Cisco Firepower Management Center access, VPN pre-shared key or certificate material.

METHOD OF PROCEDURE

1. Export and back up the current Palo Alto and Firepower rule bases before making changes.
2. Define IKE Phase 1 and IPsec Phase 2 parameters (encryption, authentication, DH group, lifetime) matching the remote site's device.
3. Configure the tunnel interface and IKE/IPsec gateway objects on the Palo Alto NGFW.
4. Assign the tunnel interface to the appropriate security zone.
5. Create scoped security policy rules permitting only the required traffic between the new site and core network zones.
6. Commit the configuration and bring the tunnel up; confirm Phase 1 and Phase 2 negotiation succeeds.
7. Review existing broad rules against logged traffic over the prior monitoring period; identify rules safe to scope down.
8. Apply narrowed rules in a controlled order, monitoring traffic logs after each change for unexpected drops.
9. Mirror equivalent policy tightening on Cisco Firepower where the same traffic paths apply.
10. Document final rule set and tunnel configuration for the change record.

TEST / VERIFICATION PLAN

- Verify IPsec tunnel shows Up/Active on both Phase 1 and Phase 2
- Verify traffic from the new site reaches required core resources

- Verify no legitimate traffic is unexpectedly dropped after policy tightening
- Review logs for a defined monitoring window post-change to confirm stability

ROLLBACK PLAN

- Disable the new tunnel interface and associated security policy rules
- Restore the prior rule base from the pre-change backup
- Confirm previously-working traffic flows are restored
- Notify stakeholders that rollback is complete

Note: Change numbers and environment labels shown here are illustrative. Client-identifying details have been withheld in accordance with a signed NDA; the process and technical steps reflect the actual change performed.