Service Brief

Firewall Deployment

Cross-Manufacturer

This document outlines the scope, deliverables, responsibilities, and terms governing Redesign's Firewall Deployment Services involving a migration between different firewall manufacturers. This engagement includes both physical deployment (installation, cabling, interface mapping) and logical configuration (policy design, routing, VPN, NAT, etc.) for each unit deployed. It is designed to replace an existing firewall with a new platform from a different vendor family.

This engagement is governed by this Service Brief and associated with SKU: FW-DIFFDEPLOY. The quantity defined in the quote reflects the number of firewalls to be physically installed and logically configured.

Table of Contents

01. Services Overview

Redesign's Cross-Manufacturer Firewall Deployment Services support the full physical and logical transition to a new firewall platform from a different vendor. This includes the review and translation of firewall policy, new device configuration, interface and routing setup, and physical replacement in a production environment. The engagement is scoped for like-for-like cutovers or site-level rollouts where network architecture remains stable. In some instances an additional SOW will be required when feature sets are enabled on the legacy firewall that are not natively supported on the new manufacturer's firewall.

02. Offer Structure

Primary Services

- Physical device installation and interface mapping
- Logical configuration of new firewall platform
- Policy translation or rebuilding from the source platform
- Routing, NAT, and VPN configuration
- Cutover coordination and go-live testing
- Post-deployment validation and configuration backup

Optional Add-Ons

Separate SOW

- Network map creation
- SIEM/logging integration
- Alternative Site-to-Site Routing and connectivity
- Branch/Remote office IPSec/ Routing

03. Project Scope

This engagement includes all activities required to remove an existing firewall and replace it with a new platform from a different vendor, such as:

- **Palo Alto, Fortinet, Cisco, CheckPoint, Sonicwall, PFsense**

Scope includes

- **Physical setup and cabling**
- **Logical configuration of interfaces, zones, policies, NAT, and VPN**
- **Pre-staging and testing prior to cutover**
- **One production cutover event per firewall**

04. Quantity & Effort Model

- Service SKU: FW-DIFFDEPLOY
- Quantity: Number of firewalls to be deployed and migrated
- Work per Unit Includes:
  - ☑ One complete firewall deployment (physical + logical)

05. Services & Key Activities

Stage	Key Activities
1. **Planning & Discovery**	☑ Gather configuration from existing device ☑ Document interface mapping and network connections ☑ Review routing, VPN, and NAT details ☑ Confirm site access or remote hands availability ☑ Identify layer 3 location and architect changes if needed
2. **Configuration & Staging**	☑ Translate policies and zones to target firewall syntax ☑ Configure interfaces, routing, NAT, and object groups ☑ Set up VPNs or tunnels as applicable ☑ Prepare device for installation (including image/firmware)
3. **Physical Installation**	☑ Rack and cable the new firewall ☑ Match interfaces to design ☑ Validate console and management access
4. **Cutover & Go-Live**	☑ Schedule and execute cutover ☑ Migrate traffic to new firewall ☑ Validate routing, VPNs, internet access, internal zones, and logs ☑ Capture fallback plan if needed
5. **Post-Deployment Validation**	☑ Perform basic application and service testing ☑ Provide final backup of config ☑ Deliver change summary and documentation

06. Deliverables

Perform basic application & service testing

Configuration Backup (final)

As-built documentation

07. Services Scope Changes

Rearchitecture, multiple migration phases, clustered deployments, or advanced traffic inspection may require a revised SOW.

08. Services Scope Exclusions

This engagement does not include:

- SIEM tuning or threat detection policy design
- Full Zero Trust or microsegmentation implementation
- Large-scale VPN user onboarding
- Configuration of undocumented or legacy devices

09. Customer Responsibilities

- Provide hardware, licenses, and rack access
- Provide access to the current firewall configuration and documentation
- Assign internal technical contact for validation and testing
- Schedule downtime or cutover windows with proper approvals

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

10. Services Schedule

- **Start Date:** Upon signed quote and receipt of configuration details
- **Completion:** Project sign-off via DocuSign from customer
- **Cutover Windows:** Must be coordinated with Redesign during business hours unless otherwise agreed

11. Terms and Conditions

This engagement will be governed by the Seller's terms and conditions located at:

www.redesign-group.com/legal

Services will not begin until the following prerequisites are met:

- Signed quote referencing **SKU: FW-DIFFDEPLOY** and quantity
- Access to current configuration and network documentation
- Firewalls delivered and licensed
- Cutover schedule approved

Failure to meet these requirements will prevent Redesign from delivering the services outlined in this Service Brief.

[re]DESIGN

The future belongs
to the curious.