

## **Service Definition: Set Up and Migration Services**

### **Category: Cloud Support (Lot 3)**

**Specialisms: Cisco ACI/NDFC, Extreme Networks, Palo Alto, Fortinet.**

#### **1. Service Overview**

We provide expert technical leadership for the transition of legacy network and security workloads to software-defined private and hybrid cloud environments. This service covers the end-to-end setup of Cisco ACI/NDFC or Extreme Networks fabrics, alongside the initial configuration of Palo Alto or Fortinet Next-Generation Firewalls (NGFW). Automation tooling such as Ansible will be used during setup phases. Using an Infrastructure as Code (IaC) approach, ensures setups & some migration services are repeatable & free from manual errors.

#### **2. Service Features**

- Fabric Architecture Design: Strategic design of Cisco ACI, NDFC, or Extreme Networks fabric topologies.
- Automated Migration: Scripted transition of legacy VLANs/workloads to software-defined fabrics.
- Security Policy Provisioning: Initial setup of Zero Trust zones and micro-segmentation rules.
- Firewall Configuration: Expert deployment of Palo Alto (Panorama) and Fortinet (FortiManager).
- Validation & Assurance: Rigorous post-migration testing to ensure operational readiness.
- System Integration: Seamless linking of new fabrics with existing cloud or on-prem assets.
- Infrastructure as Code (IaC): Use of Terraform/Ansible for repeatable, error-free deployments.
- Discovery Audits: Detailed assessment of current "as-is" network state before migration.
- SD-WAN Integration: Setup of secure edge connectivity during the migration phase.
- Knowledge Transfer: Technical handover workshops for internal operations teams.

#### **3. Service Benefits**

- Reduced Deployment Time: Faster project completion via automated fabric orchestration.
- Minimized Business Risk: Expert-led planning prevents downtime during complex migrations.
- Enhanced Security: Secure-by-design implementation using NGFW and micro-segmentation.
- Cost Efficiency: Optimized resource utilization through software-defined architecture.
- Operational Agility: Faster scaling of resources following a successful fabric setup.
- Compliance Assurance: Alignment with UK Government Cyber Essentials and NCSC guidelines.
- Reduced Complexity: Simplified management via centralized control planes (APIC/Panorama).
- Vendor Objectivity: Expert guidance on selecting the best fabric (Cisco vs. Extreme).
- Improved Visibility: Full auditability of network traffic from day one of go-live.
- Future-Proofing: Deployment of extensible architectures ready for hybrid-cloud growth.

#### **4. Onboarding and Offboarding**

##### **Onboarding (Implementation Plan)**

Our onboarding process typically spans 15 days:

Kick-off (Day 1-2): Scope validation and stakeholder alignment.

- Discovery (Day 3-7): Automated audit of existing networking and security policies.
- Secure Access (Day 8-10): Establishment of remote management links and monitoring tools.
- Baseline Handover (Day 11-15): Confirmation of the migration roadmap and service start.

##### **Offboarding (Exit Strategy)**

We ensure a clean exit with zero vendor lock-in:

- Technical Handover: Transfer of all configuration files, topology diagrams, and IaC scripts.
- Briefing Sessions: Final knowledge transfer for the successor team.
- Data Deletion: Secure purging of all client management data and credential revocation.

#### **5. Technical Requirements**

- Hardware: Buyers must own/procure the physical switches and firewall appliances.
- Licensing: Active vendor support (SmartNet/FortiCare) must be maintained by the buyer.
- Remote Access: Persistent, secure VPN access to management controllers is required.