BLACKBIRD FOR TRAINING

Network Operations and Troubleshooting Course: Cisco ACI, SD-WAN, Catalyst Center, F5 and Palo Alto



Network Operations and Troubleshooting Course: Cisco ACI, SD-WAN, Catalyst Center, F5 and Palo Alto

Introduction:

Network operations and troubleshooting is the daily work of keeping data centre fabrics, wide-area links, application delivery controllers and firewalls healthy, and of isolating and fixing faults when services fail. This one-week course is for network, data centre, WAN and firewall engineers, NOC and SOC operations staff, infrastructure architects and team leads, and each delegate leaves with a multi-vendor troubleshooting runbook. It is an advanced, intensive course for engineers who already know the basics of Cisco ACI, Cisco Catalyst SD-WAN, Cisco Catalyst Center, F5 BIG-IP and Palo Alto Networks firewalls, taught through daily hands-on labs.

Course Objectives:

- Interpret Cisco ACI faults, events, health scores and zoning rules to isolate endpoint, contract and L3Out failures in an operating fabric
- Distinguish control-plane from data-plane failures in Cisco Catalyst SD-WAN and apply centralised and localised policy and security features correctly
- Apply Cisco Catalyst Center Assurance health views, path trace and intelligent capture to locate the cause of a reported user or application issue
- Compare F5 BIG-IP LTM load-balancing, persistence and monitor options and select an F5 Advanced WAF policy approach for a given application
- Apply PAN-OS packet-flow knowledge, counters and packet captures to separate routing, NAT, policy and App-ID causes of dropped traffic
- Justify a cross-platform isolation sequence and record it as a runbook that operations teams can follow during an incident

Target Audience:

- Data centre network engineers who operate Cisco ACI fabrics and decide whether a fault lies in the policy model, the access policies or the physical fabric
- WAN and branch network engineers who run Cisco Catalyst SD-WAN overlays and judge which policy, tunnel or controller condition is degrading an application
- Network security and firewall engineers who manage F5 Advanced WAF and Palo Alto Networks firewalls and decide whether a block is a true attack or a policy error
- NOC and SOC operations staff who triage alerts from Cisco Catalyst Center and other consoles and choose which team and platform to escalate to
- Infrastructure architects and operations team leads who own troubleshooting standards and decide which isolation steps belong in a shared runbook



Course Outline:

Day 1: Cisco ACI Operations and Troubleshooting: Fabric, Policy Model and Endpoints

- APIC GUI, CLI and Moquery: Reading Managed Objects During Fabric Operations
- Faults vs Events vs Audit Logs: Tracing What Changed and When
- Health Scores and Fabric Discovery: Diagnosing Leaf, Spine and Controller Issues
- Endpoint Learning and Contracts: Verifying Zoning Rules Between Endpoint Groups
- L3Out, SPAN and Atomic Counters: Isolating External Routing and Packet Loss

Day 2: Cisco Catalyst SD-WAN Operations, Troubleshooting, Advanced Policy and Security

- SD-WAN Manager, Controller and Validator: Control-Plane Onboarding and Certificate Faults
- OMP, TLOC and BFD Sessions: Verifying Overlay Routes and Tunnel Health
- Centralised vs Localised Policy: Topology, Application-Aware Routing and QoS Behaviour
- Enterprise Firewall, IPS and URL Filtering: Securing Direct Internet Access Branches
- SD-WAN Best Practices: Template Hygiene, Upgrade Sequencing and Monitoring Baselines

Day 3: Cisco Catalyst Center Implementation and Administration for Assurance

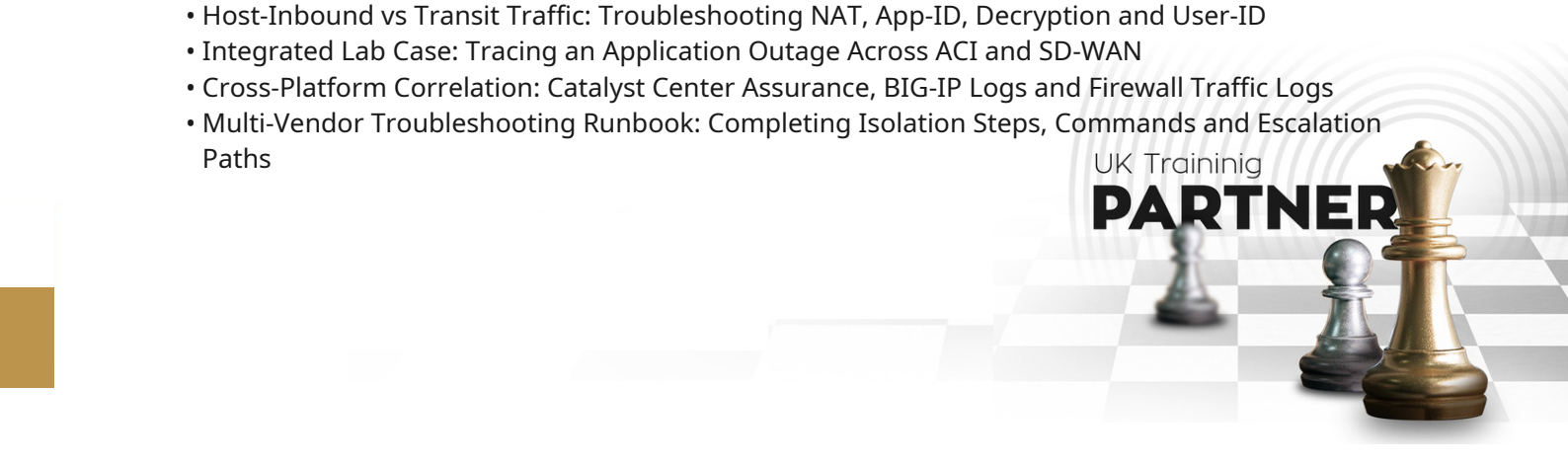
- Catalyst Center Architecture and Discovery: Inventory, Sites and Device Provisioning Prerequisites
- Network Health vs Client Health: Interpreting Assurance Dashboards and Scores
- Assurance Issues and AI-Driven Insights: Prioritising Recurring Wired and Wireless Problems
- Path Trace, Sensor Tests and Intelligent Capture: Proving Where Experience Degrades
- Assurance Administration: Thresholds, Notifications, Role-Based Access and Integration Settings

Day 4: F5 BIG-IP LTM Configuration and F5 Advanced WAF Configuration

- BIG-IP LTM Virtual Servers, Pools and Monitors: Building Resilient Application Delivery
- Persistence vs Load-Balancing Methods: Profiles, SNAT and SSL Offload Decisions
- iRules and High Availability: Traffic Steering Logic and Device Group Failover
- Positive vs Negative Security Model: Advanced WAF Policy Builder and Signatures
- Advanced WAF Tuning: Learning Suggestions, Bot Defence and False Positive Handling

Day 5: Palo Alto Networks Firewall Troubleshooting and Integrated Multi-Vendor Lab Case

- PAN-OS Packet Flow, Counters and Packet Captures: Locating the Drop Stage
- Host-Inbound vs Transit Traffic: Troubleshooting NAT, App-ID, Decryption and User-ID
- Integrated Lab Case: Tracing an Application Outage Across ACI and SD-WAN
- Cross-Platform Correlation: Catalyst Center Assurance, BIG-IP Logs and Firewall Traffic Logs
- Multi-Vendor Troubleshooting Runbook: Completing Isolation Steps, Commands and Escalation Paths



Skills You Will Gain:

- APIC Fault Analysis
- Zoning Rule Verification
- SD-WAN Overlay Diagnostics
- Assurance Data Interpretation
- Application Delivery Configuration
- Web Application Firewall Tuning
- PAN-OS Packet Flow Analysis
- Cross-Platform Fault Isolation

Why Attend This Course:

- From reacting to individual console alarms to reading ACI and Catalyst Center health data as evidence of where a fault sits
- From editing SD-WAN and firewall policies by trial and error to predicting how each policy will act before it is pushed
- From relaxing WAF policies to stop user complaints to tuning signatures and learning suggestions with a recorded reason for each change
- From escalating incidents between vendor teams without evidence to following a multi-vendor troubleshooting runbook with defined isolation steps

Conclusion:

Operating a multi-vendor network well means turning alarms from many consoles into one ordered line of evidence that points to the failing layer. The course makes clear the difference between policy faults and fabric or tunnel faults, between control-plane and data-plane symptoms, and between a genuine attack and a misconfigured security policy. It suits engineers and operations staff who already run Cisco, F5 and Palo Alto Networks platforms day to day and now need faster, repeatable isolation across all of them during live incidents.

Frequently Asked Questions FAQ:

What should engineers know before joining this Network Operations and Troubleshooting Course?

Delegates should already configure at least two of the covered platforms at basic level and be comfortable with routing, switching, TCP/IP and command-line work. The course does not teach initial installation; it assumes working knowledge and moves straight into operations, faults and isolation in labs.



How does this Network Operations and Troubleshooting Course differ from a single-vendor implementation course?

It focuses on operating and repairing platforms that already run, across several vendors, rather than building one platform from scratch. Each day covers the faults and checks that matter most, and the final day joins them into one cross-platform incident.

Why is network operations and troubleshooting harder across Cisco ACI, SD-WAN, F5 and Palo Alto platforms?

Each platform hides faults behind its own policy model, logs and terminology, so a single outage can look like four separate problems. Without an agreed isolation order, teams test the same layers repeatedly and escalate between vendors without evidence.

What do delegates take back to work from this Network Operations and Troubleshooting Course?

Delegates take back a multi-vendor troubleshooting runbook listing isolation steps, key commands, log sources and escalation points for each platform, plus lab experience applying it to a realistic outage that crosses the data centre, WAN, application delivery and firewall layers.

