JUPITER PRIME

Consulting • Training • Advisory

جوبيتر برايم للاستشارات والتدريب

COURSE BROCHURE

Advanced Secure Enterprise Network Design and Defence Course

jupiterprime.uk

info@jupiterprime.uk

Registered in the United Kingdom and Saudi Arabia

Advanced Secure Enterprise Network Design and Defence Course

Secure Enterprise Network Design and Defence is a 2-week advanced training course for network technicians and junior security practitioners moving from keeping networks running to keeping attackers out, and it ends with a segmented enterprise network blueprint built in a lab. Flat networks still let a single infected laptop reach payroll servers and plant controllers, so topology choices now decide how far an intrusion spreads. Jupiter Prime Training runs this course for practitioners making that move into network defence.

Why Secure Enterprise Network Design and Defence Matters Now

Three changes reshape the network practitioner's role: the merging of office, cloud and operational technology traffic on shared infrastructure, the rise of remote and wireless access that dissolves the old perimeter, and security teams that now expect network staff to supply telemetry and contain incidents rather than simply restore connectivity. Organisations whose networks are zoned, monitored and documented can isolate an outbreak in minutes; those with flat, undocumented designs face shutdowns that spread across sites. The course aligns design and monitoring choices with the Protect and Detect functions of the NIST Cybersecurity Framework 2.0 NIST CSF 2.0.

Who Gains Most from Secure Enterprise Network Design and Defence

- Network technicians who configure switches, routers and wireless controllers day to day
- Junior security practitioners who need a working grasp of how traffic actually flows
- Infrastructure support staff who handle site moves, new branches and campus extensions
- NOC operators who watch link health and are now asked to spot suspicious traffic
- Systems staff who manage directory, DNS and DHCP services the network depends on

A network operations team that sends technicians and its newest security staff together gains most, because both sides learn to read the same diagrams and alerts.

Secure Enterprise Network Design and Defence Capabilities

Participants leave able to draw, build and watch a network whose structure itself slows an attacker down.

- Design addressing plans and trust zones that separate users, servers and critical systems — network architects and owners
- Apply routing and switching controls that prevent spoofing and loops — network operations
- Specify firewall placement, VPN types and access policies between zones — security engineering
- Build wireless and port-based access control for staff, guests and devices — facilities and IT support
- Test intrusion detection and flow monitoring coverage across the design — security operations centre
- Communicate a network design and its residual exposures through clear diagrams — managers and auditors

Key Secure Enterprise Network Design and Defence Terms

- Trust zone — A group of network segments sharing the same security level, with traffic between zones controlled and inspected.
- VLAN — A virtual local area network that splits one physical switch fabric into separate broadcast domains for different groups.
- Network access control — Checks a device and user before allowing a network connection, often using port-based authentication.
- Demilitarised zone — A buffer segment holding internet-facing services, separated from both the internet and the internal network.
- Flow record — A summary of a network conversation listing source, destination, ports and volume, used for monitoring and investigations.
- East-west traffic — Communication between systems inside the network, where attackers move after the first compromise.

Secure Enterprise Network Design and Defence Day by Day

Day 1: How Networks Are Attacked

- OSI and TCP/IP Layers Under Attack — Where Each Threat Strikes
- Flat Network Breach Cases — Cost of Missing Segmentation
- NIST CSF 2.0 Protect and Detect Functions — Network Practitioner Duties
- Network Documentation and Diagram Standards — Visibility Before Change
- Lab Topology Introduction — Starting Network for the Blueprint

Day 2: Addressing and Core Services

- IPv4 and IPv6 Addressing Plans — Room for Zones and Growth
- DHCP Snooping and Rogue Server Prevention — Trusted Address Assignment
- DNS Security and Filtering — Blocking Malicious Domains Early
- Network Time and Directory Dependencies — Reliable Authentication and Logs
- IP Address Management Records — Accountability for Every Subnet

Day 3: Switching Security

- VLAN Design and Trunk Pruning — Limiting Broadcast and Hopping
- Spanning Tree Protection Features — Preventing Loops and Hijack
- Port Security and MAC Limiting — Unauthorised Device Control
- Dynamic ARP Inspection — Stopping Man-in-the-Middle Attacks
- Private VLANs — Isolating Hosts Within One Segment

Day 4: Routing Security

- OSPF Authentication and Area Design — Trusted Route Exchange
- BGP Filtering and Prefix Controls — Internet Edge Protection
- Access Control Lists on Routers — Coarse Filtering Between Sites
- Unicast Reverse Path Forwarding — Anti-Spoofing at the Edge
- Management Plane Separation — Out-of-Band Administration Choices

Day 5: Segmentation and Trust Zones

- Zone Model Design — Users, Servers, Guests and Critical Systems
- Demilitarised Zone Placement — Internet-Facing Service Isolation
- Operational Technology Segmentation — Protecting Plant and Building Systems
- Micro-Segmentation Options — Controlling East-West Traffic
- Inter-Zone Traffic Matrix — Documented Allowed Flows

Day 6: Firewalls and Secure Remote Access

- Next-Generation Firewall Placement — Perimeter and Internal Inspection Points
- Application-Aware Policies — Rules by Service Not Port
- Site-to-Site IPsec Tunnels — Branch Connectivity Design
- Remote Access VPN and Client Posture Checks — Teleworker Exposure
- Zero Trust Access Brokers — Alternatives to Full Network Tunnels

Day 7: Wireless and Network Access Control

- WPA3 Enterprise Configuration — Strong Wireless Authentication
- 802.1X Port-Based Authentication — Wired and Wireless Admission
- Guest and IoT Onboarding — Isolated Networks for Untrusted Devices
- Wireless Intrusion Detection — Rogue and Evil Twin Access Points
- Retail and Hospitality Wireless Cases — Sector Design Lessons

Day 8: Intrusion Detection and Prevention

- Sensor Placement Strategy — Coverage of Zones and Choke Points
- Signature-Based Detection with Snort — Known Attack Patterns
- Behavioural Detection with Zeek — Protocol Anomalies and Metadata
- Inline Prevention Versus Passive Detection — Availability Trade-Offs
- Alert Triage Workflow — Escalation to Security Operations

Day 9: Network Monitoring and Response

- NetFlow and IPFIX Collection — Visibility of East-West Traffic
- Baseline Traffic Profiles — Spotting Unusual Volumes and Destinations
- Syslog Centralisation from Network Devices — Configuration Change Evidence
- Network Containment Actions — Quarantine VLANs and Port Shutdown
- Manufacturing and Utility Incident Cases — Lessons from Network Isolation

Day 10: Practising the Segmented Enterprise Network Blueprint

- Zone and Addressing Design Applied to the Lab — Documented Trust Boundaries
- Switching, Routing and Firewall Build — Controls Enforced Between Zones
- Access Control and Wireless Configuration — Device Admission Tested
- Simulated Intrusion and Detection Check — Sensor and Flow Coverage Verified
- Segmented Enterprise Network Blueprint Completion — Diagrams, Policies and Monitoring Plan

Applying Secure Enterprise Network Design and Defence After the Course

- Map current traffic between user, server and critical system segments using flow records and propose a first inter-zone traffic matrix
- Enable DHCP snooping, dynamic ARP inspection and port security on one access switch stack and record the effect on rogue devices

Secure Enterprise Network Design and Defence Questions FAQ

What is secure enterprise network design and defence and why does it matter now?

Secure enterprise network design and defence is the practice of structuring, controlling and monitoring a network so attacks are slowed, detected and contained. It matters now because office, cloud and plant traffic share infrastructure, and flat networks let one infection spread everywhere.

Which roles gain most from secure enterprise network design and defence training?

Network technicians, junior security practitioners, NOC operators and infrastructure support staff gain most. You benefit if you configure switches and routers today and are expected to take on segmentation, monitoring and containment duties.

How does secure enterprise network design and defence training differ from a basic networking course?

It assumes you already configure network devices and adds the security design layer on top. You work on trust zones, access control, intrusion detection and containment rather than learning cabling, basic routing or device set-up.

What do you bring back from secure enterprise network design and defence training?

You bring back a segmented network blueprint built and tested in the lab. It includes zone diagrams, addressing, allowed flows, access policies and a monitoring plan you can adapt to your own sites.

Secure Enterprise Network Design and Defence: The Way Forward

The segmented enterprise network blueprint first informs which zones and inter-zone rules the next network change introduces. Network technicians build from it, security staff tune sensors against it and managers use its diagrams for approvals. After the first segmentation change, revisit the traffic matrix, since real flows usually reveal dependencies the design missed.