



Network Security Training Course: Firewalls, VPN, IDS/IPS and NAC



Network Security Training Course: Firewalls, VPN, IDS/IPS and NAC

Introduction:

Network security training covering firewalls, VPN, IDS/IPS and NAC is a 10-day course for network engineers, security engineers and firewall administrators that ends with a Segmented Network Security Design and Audit Pack. Organisations often run flat networks, ageing rule bases full of permissive entries and untuned sensors, so an intruder who passes the perimeter moves freely and goes unnoticed. Nominees already configure routers, switches or firewalls, and each day is taught as a hands-on lab on vendor-neutral and open-source tools. CoreConcept Training Center delivers this network security course.

Course Objectives:

- Map network attack paths and design security zones, DMZ placement and micro-segmentation policies that follow zero trust principles
- Build and maintain firewall rule bases and NAT on stateful and next-generation firewalls in line with NIST SP 800-41 guidance
- Configure site-to-site IPsec and TLS remote-access VPNs with certificate and multi-factor authentication
- Deploy and tune Snort or Suricata IDS/IPS sensors and Zeek monitoring to reduce false positives while keeping detection coverage
- Enforce IEEE 802.1X network access control, wireless protection and switch and router hardening based on CIS Benchmarks
- Audit network device configurations, scan devices for vulnerabilities and run change control that keeps firewall policy and baselines current

Target Audience:

- Network engineers responsible for designing and changing routed, switched and wireless enterprise networks
 - Security engineers responsible for perimeter controls, VPN gateways and intrusion detection sensors
 - Firewall administrators responsible for rule base changes, NAT and periodic policy reviews
 - Infrastructure operations staff responsible for hardening, patching and administering network devices
 - Technical assurance staff responsible for reviewing network device configurations and change records
-

Course Outline:

Day 1: Network Threat Landscape and Secure Architecture Principles

- Network Attack Paths From Reconnaissance to Lateral Movement
- Spoofing, Sniffing and Man-in-the-Middle Attack Techniques
- Defence in Depth Layers Across Perimeter, Core and Endpoint
- Wireshark Capture of Attack Traffic in a Lab
- Current-State Network Security Baseline and Exposure Map

Day 2: Segmentation, Security Zones, DMZ and Zero Trust Design

- Security Zone Model With Trust Levels and Conduits
- DMZ Placement Options for Public-Facing Services
- VLAN and VRF Segmentation Versus Micro-Segmentation Policies
- Zero Trust Principles Applied to Internal Network Flows
- Segmentation Matrix Mapping Permitted Flows Between Zones

Day 3: Firewall Types, Rule Base Design and NAT Lab

- NIST SP 800-41 Firewall Policy and Technology Selection
- Packet Filter, Stateful and Next-Generation Firewall Capabilities Compared
- pfSense Lab Building Interfaces, Aliases and Zone Rules
- Rule Base Ordering, Default Deny and Object Naming Conventions
- Source NAT, Destination NAT and Port Forwarding Configuration

Day 4: Site-to-Site and Remote-Access VPN Lab

- IPsec Tunnel Modes, ESP and Security Associations
- IKEv2 Negotiation Proposals With Pre-Shared Keys Versus Certificates
- Site-to-Site IPsec Tunnel Build Between Two pfSense Gateways
- TLS Remote-Access VPN With Multi-Factor User Authentication
- Split Tunnelling Decisions and VPN Troubleshooting With Captures

Day 5: Week-One Case Study on Firewall Rule Review and Clean-Up

- Rule Usage Analysis With Hit Counts and Firewall Logs
 - Shadowed, Redundant and Overly Permissive Rule Identification
 - Any-Any Rule Remediation and Least Privilege Rewrites
 - Rule Recertification Workflow With Business Owners and Expiry
 - Week-One Segmented Perimeter Design Review and Peer Critique
-

Day 6: IDS/IPS Deployment and Tuning With Snort and Suricata

- Network IDS Versus Host IDS Sensor Placement Choices
- Inline IPS Versus Passive Tap and SPAN Deployment
- Suricata Rule Syntax, Variables and Rule Set Management
- Signature Tuning, Thresholds and False Positive Suppression
- Zeek Network Security Monitoring Logs for Protocol Analysis

Day 7: Network Access Control, IEEE 802.1X and Wireless Security

- IEEE 802.1X Supplicant, Authenticator and Authentication Server Roles
- RADIUS Policies With EAP-TLS and Certificate-Based Device Identity
- MAC Authentication Bypass and Guest Onboarding for Unmanaged Devices
- Posture Assessment and Quarantine VLAN Enforcement Rules
- Enterprise Wireless Protection With Rogue Access Point Detection

Day 8: Device Hardening, Secure Administration, DNS and Email Gateways

- CIS Benchmarks Applied to Switch and Router Configurations
- Port Security, DHCP Snooping and Dynamic ARP Inspection
- SSH, SNMPv3 and Out-of-Band Management Network Design
- DNS Filtering, Resolver Hardening and DNS Tunnelling Detection
- Email Security Gateway With SPF, DKIM and DMARC Checks

Day 9: Network Logging, Vulnerability Scanning, Change Control and Configuration Audit

- Syslog and NetFlow Collection for Network Detection Use Cases
- Nmap and OpenVAS Vulnerability Scanning of Network Devices
- Firewall Change Request, Risk Rating and Approval Records
- Configuration Baseline Drift Checks Against Approved Device Templates
- Network Security Metrics for Rule Hygiene and Patch Latency

Day 10: Capstone Lab Building and Auditing a Segmented Network

- Capstone Lab Zone Design and pfSense Policy Implementation
 - Capstone Lab IPsec Tunnel and Remote-Access Gateway Configuration
 - Capstone Lab Suricata Sensor and 802.1X Access Control
 - Capstone Lab Configuration Audit Against CIS Benchmarks
 - Segmented Network Security Design and Audit Pack Completion
-

Skills You Will Gain:

- Security Zone Design
- Firewall Rule Base Management
- VPN Gateway Configuration
- Intrusion Signature Tuning
- Port-Based Access Control
- Network Device Hardening
- Network Vulnerability Assessment
- Configuration Audit Practice

Why Attend This Course:

- Hand the network security lead a Segmented Network Security Design and Audit Pack covering zones, firewall policy, VPN, sensors, access control and audit findings
- Decide which firewall rules to retire, where to place IDS/IPS sensors and when inline prevention is safe to enable
- Avoid breaches, audit findings and outages caused by permissive rules, untuned sensors and unhardened switches and routers
- Pass rule review checklists, hardening baselines and pfSense and Suricata lab configurations to colleagues who run the network

Conclusion:

Back at work, the participant gives the network security lead and the change advisory board a Segmented Network Security Design and Audit Pack containing a zone and flow matrix, firewall and VPN policy, IDS/IPS and 802.1X settings, hardening baselines and audit findings. The lead uses it to decide which flat segments to split first, which firewall rules to retire and where to place sensors. After the first rule recertification cycle or sensor tuning period, the team should review removed rules, false positive rates, blocked device attempts and open audit findings against the pack.

Frequently Asked Questions FAQ:

What should participants know before the network security training course on firewalls, VPN and IDS/IPS?

Participants should already configure routers, switches or firewalls and understand IP addressing, routing, VLANs and TCP and UDP ports. Command-line familiarity helps, because every day includes hands-on lab work on pfSense, Suricata, Wireshark and other open-source tools.

How does this network security training course differ from a networking fundamentals or security operations course?

It assumes participants can already build networks and teaches them to secure them through segmentation, firewall rules, VPN, IDS/IPS, NAC and hardening. Fundamentals courses teach addressing and routing, while security operations courses focus on alert triage and incident response rather than engineering controls.

Is a next-generation firewall enough for network security without IDS/IPS and NAC?

No. A next-generation firewall controls traffic between zones, but it does not see every internal flow, authenticate devices at the switch port or replace tuned intrusion sensors. Layered controls, segmentation and regular rule review add the depth an attacker inside the perimeter must overcome.

What does a participant take back from the network security training course on firewalls, VPN, IDS/IPS and NAC?

Each participant takes back a Segmented Network Security Design and Audit Pack with a zone and flow matrix, firewall and VPN policy, IDS/IPS and 802.1X settings, hardening baselines and capstone audit findings, ready to adapt to their own network.
