
Cisco ASA Firewall & Palo Alto NGFW

About This Training

Target Audience: Network Engineers, Security Engineers, SOC/NOC Professionals, Cyber-Security Students

Level: Beginner → Professional (Hands-on, Real-World Oriented)

Total Duration: 8-12 Weeks (*Flexible version also included below*)

Curriculum

| # | Topic | Description |
|---|---|--|
| 1 | Cisco ASA Firewall (ASA OS, ASDM, Firepower) | opic Details ASA Architecture Hardware Models, ASA OS Overview, Licensing ASA Modes Routed vs Transparent, Policy Modeling Initial Configuration Console access, Basic Setup, Management Access ☐ Labs Console login & basic configuration Configure inside/outside interfaces |
| 2 | ASA Management & Administration | ASDM vs CLI GUI/CLI comparison, installation, access User/AAA Local & RADIUS/TACACS authentication Backups Startup/Running config backup/restore ☐ Labs ASDM installation & HTTPS remote access AAA integration with RADIUS |

| # | Topic | Description |
|---|--|--|
| 3 | Access Control & Security Policies | Access Rules ACLs, Object Groups, Ports, NAT-exempt Stateful Inspection Connection Table, TCP/UDP inspection Threat Detection Scanning, DoS protection ☐ Labs Create ACL policies Implement object groups & service groups |
| 4 | NAT (Static, Dynamic, PAT) | NAT Types Static NAT, Dynamic NAT, PAT Twice NAT/Policy NAT When to use policy NAT Real World Scenarios Server publish, internet access models ☐ Labs Internet access through PAT Host publishing using Static NAT |
| 5 | VPN & Remote Access | IPSec Site-to-Site VPN IKE Phases, Transform Sets Remote VPN AnyConnect, SSL VPN Troubleshooting Debug, Logs, Packet capture ☐ Labs Configure Site-to-Site VPN between two ASAs Deploy SSL VPN + AnyConnect user access |
| 6 | High Availability & Failover | Active/Standby Sync, failover recovery test Active/Active Multi-context environments Health Monitoring Link/Unit failover logic ☐ Labs Configure Active-Standby failover setup |
| 7 | Firepower & IPS (Optional Advanced) | Firepower Architecture FMC, FTD vs ASA, Sensor deployment IPS + URL Filtering Signatures, Malware defense Logging & Monitoring Syslog, SNMP, NetFlow, Monitoring ☐ Labs Policy tuning in FMC IPS threat log analysis |
| 8 | Palo Alto Next-Generation Firewall (PAN-OS) | PAN-OS Architecture Dataplane/control-plane, ASIC, features Licensing Threat Prevention, URL Filtering, TP, GP Web-UI, CLI, Panorama Configuration path overview ☐ Labs Initial device setup & GUI familiarization |

| # | Topic | Description |
|----|---|---|
| 9 | Networking & Interface Configuration | Virtual Routers, Zones, VLANs L3/L2/Tap modes Routing Static, OSPF, BGP, Redistribution ARP, Routing table behaviour Flow logic ☐ Labs Create security zones & interface profiles Static route configuration |
| 10 | Security Policies & NAT | App-ID, User-ID, Content-ID App signatures, user mapping Security Policy Rule Base Layer 7 control, objects, QoS NAT Policies Source NAT, Destination NAT, Bi-Directional NAT ☐ Labs Create policies using App-ID Implement NAT translation rules |
| 11 | Threat Prevention & URL Filtering | IPS/IDS Vulnerability signatures Antivirus/Anti-spyware Sandbox & WildFire URL Categories Allowed/blocked groups ☐ Labs Create URL filtering & malware protection security profiles |
| 12 | VPN & GlobalProtect | IPSec Site-to-Site Crypto profiles, IKE proposals GlobalProtect Portal/Gateway, Certificates MFA Integration Azure/AD/LDAP SSO ☐ Labs GlobalProtect remote user VPN IPSec VPN with Cisco router/ASA |
| 13 | High Availability & Panorama | HA Modes Active/Passive & Active/Active Sync Path monitoring, preemption Panorama Template stacks, distributed deployment ☐ Labs Configure HA pair failover Template push from Panorama |

Fees

Regular: Tk. 16,000.00

Current: **Tk. 12,000.00**

Company Information

IVA Institute of Technology

Shawra Para, Dhaka, Bangladesh

Website: <https://iva-institute.com/>

Email: info@iva-institute.com

Contact:

Generated on: 22 May 2026, 01:01 AM

System Generated Document - IVA Institute of Technology

IVA
Institute of
Technology