CISCO SECURITY TECHNICAL CURRICULUM

Securing Networks with Cisco Firepower Next-Gen Firewall & NGIPS (SFWIPF)

Comprehensive 5-Day (40 Hours) Syllabus & Practical Hands-On Lab Blueprint

COURSE DURATION	FORMAT	TARGET AUDIENCE	PRIMARY PLATFORM
5 Days (40 Hours)	ILT / ILO	Security / Network Engineers	Cisco FTD & FMC

SCHEDULE	MODULES	HOURS	CORE FOCUS
Day 1	Modules 1 – 3	8 Hours	Architecture, Deployment Models, FMC Bootstrap & FTD Registration
Day 2	Modules 4 – 5	8 Hours	Interface Modes, Routing, NAT Engines, and Access Control Policies (ACP)
Day 3	Modules 6 – 7	8 Hours	Snort 2/3 NGIPS, Variable Sets, File Policies & AMP Threat Grid Sandbox
Day 4	Modules 8 – 9	8 Hours	Talos Security Intelligence (SI), ISE Identity Policies & SSL/TLS Inspection
Day 5	Modules 10 – 12	8 Hours	Site-to-Site/RA VPN, Active/Standby HA, Diagnostics & Troubleshooting

Day 1: Architecture, Platform Setup & Management Integration

8 Hours (4h Lecture / 4h Hands-on)

- **Module 1: Cisco Secure Firewall Threat Defense (FTD) Architecture**
  - Legacy ASA transition to Firepower & Secure Firewall Threat Defense (FTD unified image)
  - Hardware portfolios (Secure Firewall 1000, 2100, 3100, 4200, 9300) & FTDv cloud appliances
  - Management architectures: On-box Firepower Device Manager (FDM) vs. Centralized Management Center (FMC)
- **Module 2: FMC Initial Provisioning & FTD Registration**
  - FMC installation, initial configuration wizard, NTP, DNS, and Smart Licensing integration
  - FTD CLI initialization (bootstrap via console, IP assignment, manager configuration)
  - Secure channel registration: `configure manager add`, sftunnel authorization, and health checks
- **Module 3: Platform Settings & Administrative Baselines**
  - FTD Platform settings: Syslog destinations, SNMP traps, administrative access restrictions
  - System health monitoring, alert notifications, policy deployment models, and rollbacks

DAY 1 PRACTICAL HANDS-ON LABS

- **Lab 1:** Accessing and Navigating the Cisco Secure FMC Web Interface & System Settings
- **Lab 2:** Performing FTD CLI Initial Bootstrap and Registering to FMC with Pre-shared Keys
- **Lab 3:** Configuring Smart Licensing, Time Synchronization (NTP), and Platform Settings

Day 2: Interface Modes, Routing, NAT & Access Control Policies

8 Hours (4h Lecture / 4h Hands-on)

- **Module 4: Interfaces, Routing & Network Address Translation (NAT)**
  - Configuring Routed, Transparent, Inline Pair, Inline Set, and Passive Tap interface modes
  - Static routing, inter-VLAN routing, and dynamic routing protocols (OSPF, BGP) configuration
  - Firepower NAT Architecture: Auto-NAT (Object NAT) vs. Manual NAT, Dynamic PAT, Static NAT & Twice NAT
- **Module 5: FMC Object Architecture & Access Control Policy (ACP) Rules**
  - Reusable objects: Network, Port, URL, Geolocation, Application Filters, and Time Ranges
  - Access Control Policy structure: Mandatory, Default, and Monitor rule categories

- Rule matching logic, default actions, bidirectional inspection, and connection logging workflows

DAY 2 PRACTICAL HANDS-ON LABS

- **Lab 4:** Configuring Routed Interfaces, Sub-interfaces (802.1Q), and Static/Dynamic Routing
- **Lab 5:** Implementing Outbound Dynamic PAT and Inbound Static NAT Server Publishing
- **Lab 6:** Creating Granular FMC Network/Service Objects and Layer 3/4 Access Control Rules
- **Lab 7:** Testing Rule Evaluation Order, Logging Triggers, and Connection Verification

Day 3: Next-Gen IPS (Snort), File Policies & Advanced Malware Protection

8 Hours (3.5h Lecture / 4.5h Hands-on)

- **Module 6: Next-Generation Intrusion Prevention (NGIPS) with Snort**
  - Snort inspection engine fundamentals: Snort 2 multi-process architecture vs. Snort 3 multithreading
  - Cisco base intrusion policies (Connectivity over Security, Balanced, Security over Connectivity)
  - Tuning intrusion rules: Rule states (Generate Events, Drop and Generate, Disabled) and Rule Overrides
  - Variable Sets customization: Defining `$HOME_NET` and `$EXTERNAL_NET` parameters
- **Module 7: File Inspection Policies & AMP / Cisco Threat Grid**
  - File Policy rule actions: Detect Files, Block Files, Block Malware, and Malware Cloud Lookup
  - File type identification by payload signature vs. extension spoofing (True Type detection)
  - AMP cloud lookup, SHA-256 fingerprinting, dynamic sandbox submission to Threat Grid (Malware Analytics)

DAY 3 PRACTICAL HANDS-ON LABS

- **Lab 8:** Creating and Customizing a Tailored Snort Intrusion Policy and Tuning Variable Sets
- **Lab 9:** Executing Exploit Signatures, Validating Inline Drop Actions, and Viewing Intrusion Events
- **Lab 10:** Constructing File Policies to Block Executable & Archive Transfers
- **Lab 11:** Simulating Zero-Day Malware and Investigating Network File Trajectory in FMC

Day 4: Security Intelligence, Identity Policies & SSL/TLS Decryption

8 Hours (4h Lecture / 4h Hands-on)

- **Module 8: Cisco Talos Security Intelligence (SI) & Pre-Filter Policies**
  - Talos global reputation feeds: IP, URL, and DNS-based threat intelligence blocks
  - Custom blacklist and whitelist management; automated feed updates and sinkholing malicious domains
  - Pre-Filter Policies: Fastpathing trusted traffic and offloading hardware resources from deep inspection
- **Module 9: User Identity Integration & SSL/TLS Decryption**
  - Identity Sources: Cisco Identity Services Engine (ISE) via pxGrid, FMC User Agent, Active Directory LDAP
  - Passive identity tracking vs. Active authentication (Captive Portal fallback)
  - SSL/TLS Decryption policies: Outbound Resign (CA re-signing) vs. Inbound Known Key inspection
  - Handling decryption bypass for sensitive categories (Financial, Healthcare) and certificate pinning

DAY 4 PRACTICAL HANDS-ON LABS

- **Lab 12:** Enabling Talos Security Intelligence IP/DNS Feeds and Custom Drop Lists
- **Lab 13:** Integrating Active Directory via LDAP Realm and Establishing User-to-IP Mapping
- **Lab 14:** Authoring User- and Group-Based Access Control Rules
- **Lab 15:** Deploying SSL Forward Proxy Decryption with Internal Root CA and Bypass Rules

Day 5: Virtual Private Networks, High Availability & Troubleshooting

8 Hours (3.5h Lecture / 4.5h Hands-on)

- **Module 10: Site-to-Site & Remote Access VPNs**
  - Site-to-Site IPsec VPN: IKEv1 vs. IKEv2 configuration, crypto maps, and route-based VTI tunnels
  - Cisco Secure Client (AnyConnect) SSL/IKEv2 Remote Access VPN deployment via FMC
  - IP address pools, split-tunneling policies, and authentication profiles (RADIUS / Local / SAML)
- **Module 11: High Availability (HA) & Clustering Architectures**
  - Active/Standby failover prerequisites, stateful synchronization links, and MAC address assignment

- Interface monitoring, failover triggers, split-brain mitigation, and software upgrade workflows

- **Module 12: Operations, Diagnostics & Packet Analysis**
  - Unified event analysis: Connection events, intrusion events, audit logs, and custom dashboards
  - Command-line diagnostic tools: `packet-tracer`, inline `capture`, and `system support firewall-engine-debug`

DAY 5 PRACTICAL HANDS-ON LABS

- **Lab 16:** Establishing an IKEv2 Route-Based / Crypto-Map Site-to-Site VPN Tunnel
- **Lab 17:** Deploying Remote Access VPN for Cisco Secure Client with Split Tunneling
- **Lab 18:** Building an Active/Standby High Availability Pair and Testing Failover Triggers
- **Lab 19:** End-to-End Troubleshooting with CLI Packet-Tracer, Packet Captures, and FMC Logs

Certification Alignment: This 40-hour syllabus covers the foundational and intermediate operational domains aligned with **Cisco CCNP Security Core (350-701 SCOR)** and **Securing Networks with Cisco Firepower (300-710 SNCF)** certification tracks.