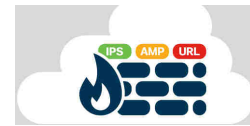


1. **Introduction to NGFW** (evolution, cyber reports, cyber kill chain)
2. **Cisco Firepower Overview**
 - a. Models and sizing (incl. hardware architecture, software flavors)
 - b. Management options and requirements
 - c. Licensing (classic vs smart)
 - d. ASA to FTD Migration
3. **Deployment Design**
 - a. First boot and installation
 - b. Routed vs Transparent Mode
 - c. BVI and L3 (routed) ports
 - d. High Availability (HA) and Clustering
4. **NGFW Traffic Control**
 - a. Packet flow and data processing
 - b. Reusable objects and object management
 - c. Routing protocols (static, OSPF, BGP)
 - d. Network Address Translation (NAT / PAT)
 - e. Pre-filter Policy (Fast-path)
 - f. Intelligent Application Bypass
 - g. Network Discovery and Host Profiling
 - h. Security Intelligence (DNS Policy, Sinkholes, DNS and IP Reputation)
 - i. SSL Policy
 - j. Preprocessors, Network Analysis and IPS
 - k. Identity Policy (Realms for AD integration, Cisco User Agent)
 - l. File control and Advanced Malware Protection (AMP)
 - m. Access Control Policy
 - n. Quality of Service (QoS) on FTD
 - o. Event Correlation and Remediation / Response
5. **System Management and Administration**
 - a. User accounts
 - b. Connections Events & Logging
 - c. Backup / Updates & Upgrades
 - d. Reporting
 - e. FlexConfig
6. **Secure Remote Connectivity**
 - a. Site-to-Site IPSec based VPN
 - b. Remote Access VPN
7. **NGFW Troubleshooting**
 - a. Tools (GUI and CLI)
 - b. Expert mode
 - c. System and NGFW services



Practical Lab exercises:

1. Cisco ASA (SFR) – basic setup in routed mode and device discovery.
2. Cisco FTDv – basic setup (On-box / FMC management) and device discovery.
3. FMCv – discovery and configuration (health policy, main settings, maintenance rules).
4. Defining reusable objects (zones, variable sets, application filters, geolocation).
5. Implementing Routing (static, OSPF, BGP).
6. Implementing static and dynamic NAT/PAT (basic and advanced).
7. Implementing and monitoring QoS on FTD.
8. Configuring and monitoring network discovery (FMC).
9. Configuring DNS Policy (ASA SFR / FMC).
10. Defining and implementing Security Intelligence (ASA SFR / FMC).
11. Defining and configuring File Inspection Policy (AMP).
12. Defining and implementing Access Control Policy (ASA SFR / FMC) with IPS.
13. Implementing and testing correlation policy and remediation actions.
14. System Administration (Scheduling tasks, Executing Backup, Audit Logs & Search, FlexConfig).
15. Reporting – generating standard and custom reports (FMC).
16. Implementing IPSec S2S VPN.
17. Configuring and implementing High Availability (HA).
18. Troubleshooting system and user traffic.