CISCO FIREPOWER next-generation Firewall - BOOTCAMP

Target audience

This course is recommended for network technicians, administrators, system integrators, security consultants and analysts, security and network operations center (SOC/NOC) personnel, solution architects and cyber security forensics specialists, who want to gain extensive knowledge about deploying and managing Firepower Threat Defence Firewalls on network edge, within data center, as VPN headend or security gateway, both in SMB and enterprise networks.

It is recommended that participants have already gathered experience with Cisco ASA firewalls, know common routing protocols and switching technologies, have good TCP/IP understanding, and ideally already worked with packet filtering technologies.

Course description

This course presents students the Cisco Firepower technology – starting with a cyber security overview, basic introduction, then going through hardware and software, setup and installation basics. Next the students learn more advanced topics like IP routing, network address translation (NAT/PAT), high availability and clustering. Course explores the NGFW features in details and students learn how to configure and implement network discovery, security intelligence, file and malware detection, next-generation IPS (Intrusion Prevention System) and secure connectivity technologies (remote access and site-to-site VPN). Students also learn and explore different troubleshooting tools necessary in daily job of the NOC/SOC engineer, i.e. for a root cause analysis or simple and complex network problem resolution (system itself and end-user traffic issues).

This course combines lecture materials with extensive hands-on labs to ensure that students can successfully deploy and manage next-generation firewall, based on Cisco Firepower technology. Lab exercises are designed in a way to finish the training on last day with fully operational NGFW deployed with available traffic control policies, very similar to real deployment scenario seen very often in the SMB or enterprise network.

Lab environment

Students work individually or in teams of two (depending on class size and delivery option) and complete up to 20 lab exercises, which are focused on discovery, configuration and tuning of different system and network parameters.

AGENDA

1. **Introduction to next-generation firewall**
   a. Evolution of the firewalls
   b. Cyber kill chain model
   c. Threats and cyber reports

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
   e. Real examples – Use Case 1

3. **Deployment Design**
   a. First boot and installation
   b. Routed vs Transparent Mode
   c. Interfaces and ports (Management, BVI, L3 routed, Inline Sets/Pairs)
   d. High Availability (HA) and Clustering
   e. Real examples – Use Case 2

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 and Restore
   d. Software Maintenance
   e. Reporting
   f. FlexConfig and Threat Defense Service Policies

6. **Secure Connectivity and Virtual Private Networks**
   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

8. **Integrations**
   a. pxGrid
   b. AMP for Endpoints
   c. Threat Intelligence Director (3rd party Intelligence Feeds)
   d. Cisco Threat Response

Practical Lab exercises:

1. Cisco ASA (SFR) – basic setup in routed mode (L3) 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. Configuration and testing of the Inline-Set interfaces (IDS/IPS).
8. Implementing and monitoring QoS on FTD.
9. Configuring and monitoring network discovery.
10. Configuration and testing DNS Policy.
11. Defining and implementing Security Intelligence.
12. Defining and configuring File Inspection Policy (AMP).
13. Defining and implementing Access Control Policy with IPS.
14. Implementing and testing correlation policy and remediation actions.
15. System Administration (Scheduling tasks, Executing Backup, Reviewing Audit Log and Search section, FlexConfig).
16. Reporting – generating standard and custom reports.
17. Implementing IPSec S2S VPN.
18. Configuring and implementing High Availability (HA) with FTD sensors.
19. Troubleshooting system and user traffic.
20. Threat Intelligence Director – implementing 3rd party intelligence feeds.