Course duration 3 days

Cisco Secure Firewall

Cisco Firepower Threat Defense Overview

Understanding firewall technology

- NGFW concept
- Different Firepower series
- NGFW features

Basic Configuration and Verification Setting

- Verify and create objects for exercise
- Modify the access control policy
- Create NAT policies
- Configure Branch1 FTD using FMC
- Configure FTD using FDM
- Deploy the Configuration changes
- Modify the network Discovery policy
- Deploy the configuration changes

NAT and Routing

- Configure static NAT
- Configure BGP

Prefilter Policies

Device Deployment with the REST API

Basic configuration using FDM

Integrated Routing and Bridging (IRB)

- Modify the NGFW interface configuration
- Modify the NAT policy
- Modify the access control policy
- Deploy and test the configuration

High Availability Configuration

- Configure and Deploy backup NGFW
- Upgrade software on backup NGFW
- Create HA pair of firewalls
- Configure Active/Standby with Virtual Mac Address

Advance Packet Flow Analysis

- Packet Tracer
- Capture with Trace

Cisco Threat Intelligence

- Upload a list of URLs to CTID that will trigger an incident
- Subscribe CTID to a TAXII feed
- Generate CTID incidents