

Cisco Next Generation Firepower Training

- Cisco Firepower Threat Defense Overview
- Firepower NGFW Device Configuration
- Firepower NGFW Traffic Control
- Firepower NGFW Address Translation
- Firepower Discovery
- Implementing Access Control Policies
- Security Intelligence
- File Control and Advanced Malware Protection
- Next-Generation Intrusion Prevention Systems
- Site-to-Site VPN
- Remote-Access VPN
- SSL Decryption
- Detailed Analysis Techniques
- System Administration
- Firepower Troubleshooting

LABS DURING THE TRAINING

Our Lab sessions focus on practical aspects for Implementing & Troubleshooting SD-Access operation of: -

- Initializing Cisco Firepower Threat Defense (FTD) on VMware Workstation
- Manage Firepower Threat Defense (FTD) through Firepower Device Manager (FDM)
- Initializing Cisco Firepower Management Centre (FMC) on VMware Workstation
- Register Cisco Firepower Threat Defense (FTD) into Management Center -Cisco FMC
- Register Cisco FMC Smart License with a token from Cisco Smart Software Manager
- Basics with Firepower Device Manager - FDM (Interface configuration, security zones)
- Basics with Firepower Management Center - FMC (Interface configuration, security zones)
- Backup and Restore
- IPv4 Static and default route
- IPv4 RIP
- IPv4 OSPF
- IPv4 EIGRP (Flex Config)
- Firepower Threat Defense-IPv6
- Firepower Threat Defense-Objects
- Firepower Threat Defense-Pre-filter rules
- Firepower Threat Defense-Access-control-Policies (ACP rules)
- Firepower Threat Defense-Platform settings
- IPv4-NAT (Network Address Translation) (Auto NAT)
- IPv4-NAT (Network Address Translation) (Manual NAT)
- Firepower Threat Defense-SLA (Service Level Agreement)

- Firepower Threat Defense-Site-to-Site VPN Ikev1
- Firepower Threat Defense-Site-to-Site VPN Ikev2
- Firepower Threat Defense-Site-to-Site VPN Ikev1 with NAT
- Firepower Threat Defense-Site-to-Site VPN Ikev2 with NAT
- Firepower Threat Defense-Site-to-Site VPN ikev1 with Cisco Router
- Firepower Threat Defense-Site-to-Site VPN ikev2 with Cisco ASA
- Remote access VPN (Cisco Any connect) with Cisco ISE
- Firepower Threat Defense-High Availability
- Next Generation Intrusion Prevention System (NGIPS)
- Discovering Network Applications and Controlling Application Traffic
- Firepower Threat Defense-Malware Policy
- Firepower Threat Defense-URL Filtering