WSFE - Cisco Web Security Field Engineer

Exam Code: 700-281

Learn to install, configure, operate and maintain Cisco Web Security products and solutions.

In this course, you will learn to install, configure, operate, manage and troubleshoot Cisco web security products. You will learn different type of deployments of web security products on Cisco IOS routers, layer3 switches and Cisco ASA Firewall.

Did You Know?

This same training is available in our ONLINE-TRAINING- live online training that builds up foundational knowledge of all the required technologies, expert instructors to ensure superior training, regardless of your location.

What you will learn

- Cisco Web Security Appliance Architecture
- Installation and deployment of different proxy modes, PAC file hosting
- Authentication based policies
- Enforcing AUC, URL filtering , Bandwidth control, AVC
- CWS (Formerly ScanSafe) Framework
- Cisco WSA in connector mode
- Cisco ASA or IOS router in connector mode.
- Managing WSA – shutdown, reboot, upgrade, license, reset, FTP, SNMP etc
- Use of delegated administrator accounts
- Policy trace, DLP, Anti-malware filtering, WRS
- Reporting, Log subscription etc

Audience

CCNA Security Certified Engineers

CCNP SITCS Certified Engineers

Prerequisites

CCNA R&S and CCNA Security

Labs

Lab1: Installing vWSA and License file
Lab2: Configuring initial setup, configuring Transparent redirection using ASA and vWSA
Lab3: Configuring Authentication Realm, Integrating with AD
Lab4: Configuring Identities, Access Policies, URL filtering, AUC
Lab5: Configuring WSA in Explicit forwarding mode, PAC file hosting.
Lab6: Configuring HTTPs proxy, Decryption policies, AVC, Bandwidth usage limit
Lab7: Configuring WCCPv2 between IOS router or L3-switch
Lab8: Policy Trace, User account creation, Log subscription
Lab9: Analyzing reports on Cisco WSA
Lab10: Configuring Cisco WSA in CWS connector mode.

