Deploying Cisco ASA VPN Solutions (642-648)

Exam Description: The 642-648 Deploying Cisco ASA VPN Solutions (VPN) exam is associated with the CCNP® Security and Cisco VPN certifications. This 90-minute, 60–70 questions, exam tests a candidate's knowledge of the skills needed to deploy Cisco ASA-based VPN solutions using ASA version 8.4. Candidates can prepare for this exam by taking the Deploying Cisco ASA VPN Solutions (VPN) course. The recommended pre-requisite exams for this exam are ICND1, ICND2, IINS, and SECURE. The exam is closed book and no outside reference materials are allowed.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

25% 1.0 ASA VPN Configuration Components

1.1 Identify ASA VPN licensing requirements
- 1.1.a AC essential
- 1.1.b AC premium
- 1.1.c AC premium shared license
- 1.1.d AC mobile
- 1.1.e Advanced endpoint assessment
- 1.1.f Flex license
- 1.1.g WSA license for AC WSA secure mobility

1.2 Identify the components and features of Any Connect 3.0 mobility (VPN, NAM, web Sec (scan safe), Telemetry)
- 1.2.a VPN
- 1.2.b NAM
- 1.2.c Web Sec (scan safe/WSA)
- 1.2.d Posture module and standalone host scan package
- 1.2.e Telemetry

1.3 Implement ASA VPN connection profiles, group policies, and user policies
- 1.3.a Policy hierarchy/Inheritance
- 1.3.b Default policies
- 1.3.c Connection profiles/group policies/user policies configurations
- 1.3.d Implement basic access control and split tunneling using ASDM
- 1.3.e Connection profile lock

1.4 Implement SCEP proxy operations using ASDM
- 1.4.a SCEP proxy solution components
- 1.4.b ASA SCEP proxy

1.5 Implement local and external VPN authorization using ASDM
- 1.5.a Local (ASA) VPN authorization
- 1.5.b VPN authorization using external policy servers
- 1.5.c ACL, web ACL, group policy restriction authorization policy

1.6 Implement VPN session accounting using ASDM
- 1.6.a VPN accounting using external RADIUS and TACACS+

1.7 Implement CSD and independent host scan operations using ASDM
- 1.7.a CSD features
- 1.7.b CSD installation and configurations and customizations
- 1.7.c Pre-Login policies, vault, cache cleaner, host emulation detection, key logger detection
- 1.7.d Pre anyconnect 3.0 host scan and post anyconnect 3.0 independent host scan
- 1.7.e Endpoint assessment
- 1.7.f Advanced endpoint assessment

1.8 Implement DAP operations using ASDM
- 1.8.a Policy hierarchy — DAP rules over user and group policies
- 1.8.b DAP features and operations
- 1.8.c Default DAP access policy
- 1.8.d DAP configurations (attributes matching and authorization parameters)
- 1.8.e DAP records aggregation
- 1.8.f Integration CSD with DAP

1.9 Implement local CA operations for SSL VPNs using ASDM
- 1.9.a ASA local CA feature and limitations
- 1.9.b ASA local CA operations and configurations

1.10 Implement certificate maps using ASDM
- 1.10.a Configure certificate mappings to match users to tunnel groups based on the certificate fields

1.11 Identify the ASA IPv6 VPN capabilities
- 1.11.a IPv6 VPN support on the ASA (8.3 IPv6 support for IKEv1 S2S VPN)

1.12 Monitor and verify the resulting CLI commands resulting from the various VPN configurations on the ASA
- 1.12.a Explain various VPN configurations CLI commands and show outputs

12% 2.0 ASA IP SEC S2S VPN

2.1 Implement a security high level design according to policy and environmental requirements by identifying Cisco ASA IPSec S2S VPN features and supporting technologies
- 2.1.a IKEv1 vs IKEv2
- 2.1.b Authentication methods

2.2 Implement basic IPSEC S2S VPN operations with PSK and digital certificates using ASDM
- 2.2.a IPSec S2S VPN configuration using PSK authentication
- 2.2.b IPSec S2S VPN configuration using certificate based authentication

2.3 Implement basic IKEv2 based IPSEC S2S VPN operations using ASDM
- 2.3.a IPSec IKEv2 based S2S VPN configuration using PSK authentication

2.4 Troubleshoot the initial provisioning IPSec S2S VPN applications due to misconfiguration
- 2.4.a Use ASDM, show and debug CLI commands to verify and troubleshoot IPSec S2S VPN operations

13% 3.0 ASA EZ VPN

3.1 Implement a security high level design according to policy and environmental requirements by identifying Cisco ASA VPN client features and supporting technologies
- 3.1.a IPSec Client
- 3.1.b AnyConnect 3.0 IPSec support
- 3.1.c IKEv1 vs IKEv2
- 3.1.d Authentication methods
- 3.1.e EZVPN servers hardware
- 3.1.f EZVPN remote hardware

3.2 Implement basic EZVPN server operations on the ASA using ASDM
- 3.2.a IKE and IPsec policy
- 3.2.b Group PSK, certificate based authentication, hybrid authentication
- 3.2.c Extended user authentication
- 3.2.d Client network settings
- 3.2.e Basic access control

3.3 Implement basic EZVPN remote operations on the ASA 5505 using ASDM
- 3.3.a Client mode vs. network extension Mode
- 3.3.b Group PSK, certificate based authentication, hybrid authentication
- 3.3.c User authentication options
- 3.3.d Remote management
- 3.3.e Device pass-through
- 3.3.f IPSec over TCP

3.4 Implement AnyConnect 3.0 IKEv2 RA VPN operations (I would remove the IPSEC client coverage to make room)
- 3.4.a AnyConnect IKEv2 IPSec RA VPN configurations
- 3.4.b AnyConnect profile editor (ASDM integrated and standalone)

3.5 Implement client services server (CSS) feature
- 3.5.a List the features enabled with client services server for AnyConnect IPSec (IKEv2) VPN

3.6 Troubleshoot the initial provisioning IPSec RA VPN applications due to misconfiguration
- 3.6.a Use ASDM, show and debug CLI commands to verify and troubleshoot IPSec EZVPN operations

13% **4.0** **ASA AnyConnect SSL VPNs**

4.1 Implement a security high level design according to policy and environmental requirements by identifying Cisco ASA anyconnect client features and supporting technologies

- 4.1.a Pre and post anyconnect 3.0 SSL VPN features
- 4.1.b Web launch versus stand-alone

4.2 Implement DTLS operations using ASDM

- 4.2.a DTLS benefits and configuration

4.3 Implement basic anyconnect 3.0 full tunnel SSL VPN operations

- 4.3.a Basic anyconnect SSL VPN configurations
- 4.3.b Web launch configurations

4.4 Troubleshoot anyconnect SSL VPN operations using DART

4.5 Implement anyconnect Profiles using ASDM

- 4.5.a Anyconnect profile options and parameters for anyconnect SSL VPN operations
- 4.5.b Anyconnect profile editor (ASDM integrated and standalone)

4.6 Implement advanced authentication in anyconnect Full Tunnel SSL VPNs (certificate/multi authentication) using ASDM

- 4.6.a External AAA authentication
- 4.6.b Certificate based authentication
- 4.6.c Advanced PKI integrations
- 4.6.d Multi authentications

4.7 Troubleshoot the initial provisioning client-based SSL VPN applications due to misconfiguration

- 4.7.a Use ASDM, show and debug CLI commands to verify and troubleshoot anyconnect SSL VPN operations

28% **5.0** **ASA Clientless SSL VPNs**

5.1 Implement a security high level design according to policy and environmental requirements by identifying Cisco ASA clientless SSL VPN features and supporting technologies

5.2 Implement basic clientless SSL VPN operations using ASDM

- 5.2.a Provision identity cert for ASA
- 5.2.b Connection profile
- 5.2.c Group policy
- 5.2.d Optional DNS settings
- 5.2.e Local user authentication

5.3 Implement advanced applications access using ASDM

- 5.3.a Advanced application deployment options
- 5.3.b Application plugins
- 5.3.c Smart tunnels

5.4 Implement the SSO features on the ASA in a clientless SSL VPN environment
- 5.4.a Basic HTTP, NTLM, and FTP SSO authentication
- 5.4.b Dedicated SSO server

5.5 Implement advanced authentication in clientless SSL VPNs (certificate/multi authentication) using ASDM
- 5.5.a Certificates issued by external CA
- 5.5.b External AAA database
- 5.5.c Multiple sequential authentication

5.6 Manage the clientless SSL VPN user interface and portal using ASDM
- 5.6.a URL entry, bookmarks, and web-type ACLs
- 5.6.b File server entries, file server browsing, hidden CIFS share access
- 5.6.c Custom home page via Smart Tunnel

5.7 Implement basic portal customization
- 5.7.a Login page
- 5.7.b Portal page
- 5.7.c Logout page
- 5.7.d Assign customization object to a connection profile

5.8 Troubleshoot the initial provisioning of clientless SSL VPN applications due to misconfiguration
- 5.8.a SSL/TLS session checking
- 5.8.b User authentication checking
- 5.8.c Connection and group profile checking

8% 6.0 SSL VPN High Availability

6.1 Implement SSL and IPSEC VPN high availability features
- 6.1.a Redundant peering
- 6.1.b Cluster load balancing
- 6.1.c Active standby failover