Deploying Cisco ASA Firewall Features (642-618)

Exam Description: The 642-618 Deploying Cisco ASA Firewall Features (FIRE) exam is associated with the CCNP® Security certification. This 90-minute, 60–70 questions exam tests a candidate's knowledge of implementing and maintaining Cisco ASA-based perimeter solutions using ASA version 8.4. Candidates can prepare for this exam by taking the Deploying Cisco ASA Firewall Features (FIRE) course. The recommended pre-requisite exams for this exam include 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.

45% 1.0 ASA Basic Configurations

1.1 Identify the ASA product family
1.1.a 5585-X
1.1.b 8.3 memory requirements
1.1.c AIP-SSC
1.1.d AIP-SSM
1.1.e CSC-SSM
1.1.f 5585-FW/VPN SSP
1.1.g 5585-IPS SSP

1.2 Implement ASA licensing
1.2.a Identify ASA licensing requirements
1.2.b Install and verify ASA license

1.3 Manage the ASA boot process
1.3.a ROMMON
1.3.b ASA 5505 factory default config

1.4 Implement ASA interface settings
1.4.a ASA interface security levels
1.4.b IP addressing, DHCP client, name, speed, duplex
1.4.c Management only interface
1.4.d VLANs
1.4.e Same security levels intra and inter interface communications

1.5 Implement ASA management features
1.5.a Basic settings (hostname, domain name, passwords, DNS)
1.5.b Passwords encryption (ASA 8.4)

1.5.c Enabling management access methods
1.5.d Management access authentication, authorization, accounting
1.5.e Privilege levels
1.5.f Local user database
1.5.g External database (ACS 4.2)
1.5.h NTP
1.5.i Logging options and netflow secure event logging
1.5.j SNMP
1.5.k DHCP server
1.5.l Managing ASA file system/configs/images
1.5.m Packet tracer
1.5.n TCP pings (ASA 8.4)

1.6 Implement ASA access control features
1.6.a Interface ACL
1.6.b Time based ACL
1.6.c Global ACL (ASA 8.4)
1.6.d Object groups
1.6.e uRPF
1.6.f Shun
1.6.g Cut-through proxy (authentication/authorization/accounting)

1.7 Implement NAT on the ASA
1.7.a Pre 8.3 – static, dynamic, policy, identity nat, nat exemption
1.7.b 8.3 – object (auto) nat, manual (twice) nat

1.8 Implement ASDM public server feature
1.8.a ASDM configurations and verify resulting CLI commands

1.9 Implement ASA QoS settings
1.9.a PQ
1.9.b Policing
1.9.c Shaping

1.10 Implement ASA transparent firewall
1.10.a Bridge group support on ASA 8.4
1.10.b Layer 3-7 access controls
1.10.c Layer 2 access controls

10% 2.0 ASA Routing Features
2.1 Implement ASA static routing
2.1.a Static routes
2.1.b Default routes

2.2 Implement ASA dynamic routing
2.2.a ASA multicast routing support
2.2.b ASA dynamic routing protocols support
2.2.c Basic EIGRP routing

25% 3.0 ASA Inspection Policy

- 3.1 Implement ASA Inspections features
  - 3.1.a Modular policy framework
  - 3.1.b Default policy and tuning
  - 3.1.c L3/L4 inspections
  - 3.1.d Advanced application inspections
  - 3.1.e ASDM UC config wizard
  - 3.1.f Connection and local host tables
  - 3.1.g TCP state bypass
  - 3.1.h TCP normalizer
  - 3.1.i Dynamic protocol support (established command)
  - 3.1.j TCP Intercept
  - 3.1.k Connection limits

5% 4.0 ASA Advanced Network Protections

- 4.1 Implement ASA botnet traffic filter
  - 4.1.a Blocking and threat level
  - 4.1.b Black and white List
  - 4.1.c Dynamic database updates
  - 4.1.d DNS inspection

15% 5.0 ASA High Availability

- 5.1 Implement ASA Interface redundancy and load sharing features
  - 5.1.a Interface redundancy
  - 5.1.b EtherChannel (ASA 8.4)

- 5.2 Implement ASA virtualization feature
  - 5.2.a Security contexts
  - 5.2.b Security contexts resource limiting

- 5.3 Implement ASA stateful failover
  - 5.3.a Active/Standby
  - 5.3.b Active/Active
  - 5.3.c Dynamic routing protocol stateful failover (ASA 8.4)