ASA Interview Questions

WWW.NETWORKINGINFO.IN

Version 1.0
Update by Dinesh Jangid

Chance to get your dream job just by preparing the interview with confidence ☺

- Last minute but fast revision
- Brush up knowledge with most likely questions and answers
- The straight and precise question to the point

1. **What is the difference between a gateway and firewall?**
   Ans – **Gateway** – Joins two different network segments. It may be software and hardware based. Example – Router, Modem, Computer

   Firewall – It Guards a network against unauthorized incoming and outgoing access. It may be Software and hardware based. Example – ASA, Checkpoint
   Note – A firewall can act as a gateway and there are many devices in the market come with both the Functionalities

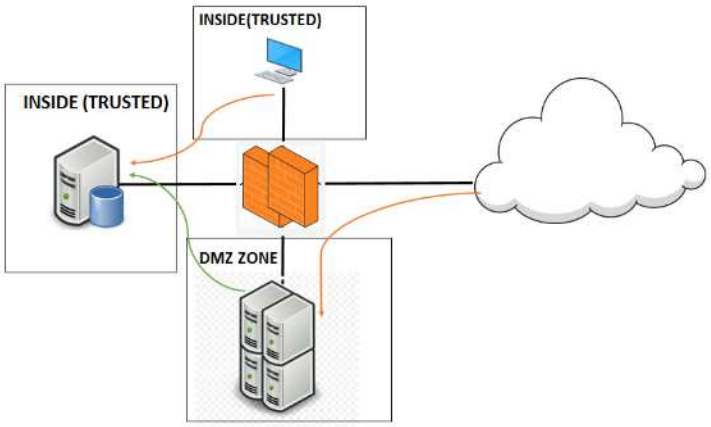
2. **What is a Stateful Firewall?**
   Ans - **Stateful Firewall** – This type of firewall is aware of the connections that pass through it. They maintain, keep track of all the connections and its state in a connection table, which is dynamically created. Example of Stateful FW – ASA, Checkpoint, PIX

   Stateless Firewall – Mostly known as a packet filtering firewall. Stateful firewalls do not look at the state of the connection but just at the packet. Always rely on source, a destination address, and services. Example of Stateless FW– Router with Access-list

3. **Stateful vs Stateless firewall, Which firewall is better in a larger business-oriented network?**
   Ans – Stateful firewall is a powerful firewall and it is better than stateless.

4. **What is default-security level for ASA outside interface?**
   Ans – security-level 0

5. **What is DMZ zone?**
   Ans – It is an intermediate zone, which may have physical or logical devices. DMZ is directly exposed to an untrusted network (Internet). Internet users can have access to the DMZ instead of having direct access to a fully trusted network.



6. **What is a denial of service?**
   Ans – **Denial of service** is a type of attack. Denial of service attack makes services unavailable. An attacker sends a bunch of requests to a server and asks for a response to such requests. Server becomes busy sending replies to the attacker, which makes server busy. All other services become unavailable due to this type of attack.
   Symptoms – performance degradation, unavailability of particular services

7. **Can you explain VPN and VPN types?**
   Ans – It is a virtual private network, which can be established on public and private networks. It is an end-to-end connection between remote private sites. VPN is not secure by default until we use additional security protocols.
   Types of VPN:
   1 **Site to Site VPN** – Always up and connects branch offices to head office. Example – IPsec
   2. **Remote Access VPN** – Not always, up. It is suitable for remote users who want to access the office network. Remote users required VPN client software to connect and access the office resources from anywhere. Example – Anyconnect, IPsec client VPN.
      Remote access has two types
      1. **Client based** – Requires VPN client software to be installed in a user's pc.
      2. **Clientless** – Requires only a web browser to connect to a secure gateway. It is also known as an SSL VPN.

8. **Common commands to troubleshoot IPSec VPN on ASA?**
   Ans:
   # Show run crypto isakmp (To see phase 1 ISAKMP configuration)
   # Show run crypto ipsec (To see phase 2 IPSec configuration)
   # Show run crypto map (To see crypto map configuration)
   # show crypto ipsec sa (To see phase 2 IPsec operational data)
   # show crypto isakmp sa (To see phase 1 ISAKMP operational data)
   # debug crypto isakmp (To see phase 1 negotiation)
   # debug crypto ipsec (To see phase 2 negotiation)
   # clear crypto ipsec (To clear phase 2 connection)
   # clear crypto isakmp (To clear phase 1 connection)

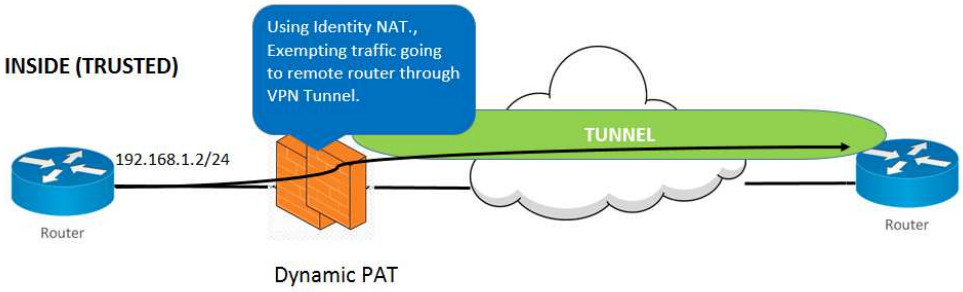
9. **How to reset all the tunnels using one command?**
   Ans - # clear crypto isakmp SA

10. **How to reset only one tunnel?**
    Ans - # clear IPsec SA peer X.X.X.X

11. **Things, which you cannot configure on ASA?**
    Ans
    1. ASA doesn't support loopback
    2. No Telnet on lowest security level interface (Need VPN)
    3. No Native VRF and MPLS

12. **What is identity NAT?**
    Ans – It is used to create a transparent mapping so that inside IP addresses appear on the outside without translation. Identity NAT is similar to NAT exemptions (NAT0). It is used to exempt traffic from being translated while passing through the VPN. In 8.3 there is no NAT 0 concept and now the term is identity NAT.

If your VPN connection is terminated on the outside interface of the ASA and you are running Dynamic PAT on that interface then all traffic passing in the direction of the Dynamic PAT means inside to outside will be matched against it and will be translated as per Dynamic PAT rule. This is one of the reasons we define identity NAT so that VPN traffic separates from normal traffic and it matches before the dynamic PAT.



Identity NAT falls into three categories

1. Dynamic Identity NAT
2. Static Identity NAT
3. Policy-based Static Identity NAT

13. How many modes do we have in ASA?

Ans – There are two modes

1. **Routed** – Default mode, which makes ASA a hop and ASA acts as a gateway.
2. **Transparent** – Makes ASA a transparent layer 2 bridge.

14. Does ASA allow traffic between same-security level configured interfaces by default?

Ans- No ASA does not.

If you want to allow, then you need to use below command

#same-security-traffic permit inter-interface

15. What is the command to check the NAT table in ASA?

Ans – show xlate

16. Which command to configure ASA into multimode

Ans - # mode multiple

17. What is Context in ASA?

Ans – Context is a virtual firewall inside a physical device.

We can partition a single security appliance into multiple virtual devices, called as security contexts.

18. Which are the features not supported in multiple context mode?

Ans:

1. Dynamic Routing Protocol
2. VPNs
3. Multicast Routing
4. Phone Proxy
5. Qos
6. Unified communication
7. Active/Standby failover

19. Which are the features supported in multiple modes?

Ans:

1. Routed and transparent mode

2. Static routing only
3. Active-Active Failover only
4. IPv6

20. What does happen when we use mode multiple command?

Ans:

1. ASA converts running-config into two files:
    1. **Startup-config** – for the system configuration
    2. **Admin.cfg** – It is used for admin context (Root dir for internal flash)
    3. Original config file of single mode is saved as old_running.cfg (root dir of internal flash). The original startup-config of the single mode is not saved.
3. The admin context is automatically added to the system configuration with the name "**admin**"
4. Context mode is not stored in the configuration
5. System Reboots

21. What is a class in context mode?

Ans: Classes provide a way of managing how much processing and hardware resources are utilized by each security context so that a single context does not overwhelm the firewall leaving the other context without any resources left to perform their function. Resources allocation is done only in system execution space (system config)

22. Can you explain admin context?

Ans – It is a context, which is automatically created when we convert single mode firewall into the multimode firewall.

23. What is the default TCP session timeout in ASA?

Ans - It's 60 Minutes

24. What is the default UDP session timeout in ASA?

Ans - It's 2 Minutes

25. What is the default ICMP session timeout in ASA?

Ans - It's 2 Seconds

26. What is the default security level in ASA?

Ans - 100

27. Difference between Transparent Firewall and Routed Firewall

Transparent Firewall - It acts as a layer 2 device.
Routed Firewall - It acts as a Layer 3 device

28. What is Stateful inspection?

Ans: It's a function of a firewall or a router where these devices keep tracks for action connection. It makes a dynamic connection table that is continuously updated with each new connection.

29. Which command is used to check the connections table?

Ans - Show conn

30. What are the types of ACLS does ASA support?

1 - Standard
2- Extended
3. Ethertype ACL (For Transparent FW)
4. Webtype ACL (For SSL VPN)

31. Features not supported in Transparent mode?

Ans:

1- Dynamic Routing
2. QOS
3. VPN like IPSec and WebVPN cannot be terminated
4. ASA can't work as a DHCP relay agent

32. What information is exchanged between ASAs over a Failover link?

1- State - Active or Standby.
2. Hello Messages
3. Network Link Status
4. Mac Addresses.
5. Configuration Replication and Synchronization.

33. What is not exchanged between ACTIVE/STANDBY?

Ans:

- DHCP Server information
- Phone proxy
- AIP module

34. What is failover hello and hold down timer?

Ans - 1 second hello and 15 seconds hold down

35. What is system IP in active standby?

Ans - It's IP address of Active FW

36. Which command to check ASA state?

Ans - #prompt hostname priority state

37. What is the system config in Context-based firewall?

Ans - This keeps basic information about all the contexts. It's doesn't' contain ACL, VPN config, etc.
Example - Name of the contexts, Port allocations, Resources allocation, Config URL,

38. What happens when you convert ASA into Multimode ASA(Context)?

Ans – 1. Once we convert ASA into Multimode then ASA copies run config to old.running.cfg
2. Creates a new context - Admin context (Copies old running-config into Admin context)
3. Associates some resources in the default class
4. Admin context gets the interfaces allocated automatically based on the old running-config

39. What is the limitation of context-based firewall?

Ans - Context based firewall doesn't support dynamic routing

40. Does ASA inspect ICMP by default?

Ans - ASA doesn't inspect ICMP by default

41. Can we switch from one context to another context?

Ans - No. You can only switch between system and admin context.