Cisco

642-617
Deploying Cisco ASA Firewall Features

Questions & Answers PDF

Question: 1

Which Cisco ASA feature enables the ASA to do these two things? 1) Act as a proxy for the server and generate a SYN-ACK response to the client SYN request. 2) When the Cisco ASA receives an ACK back from the client, the Cisco ASA authenticates the client and allows the connection to the server.

A. TCP normalizer
B. TCP state bypass
C. TCP intercept
D. basic threat detection
E. advanced threat detection
F. botnet traffic filter

Answer: C

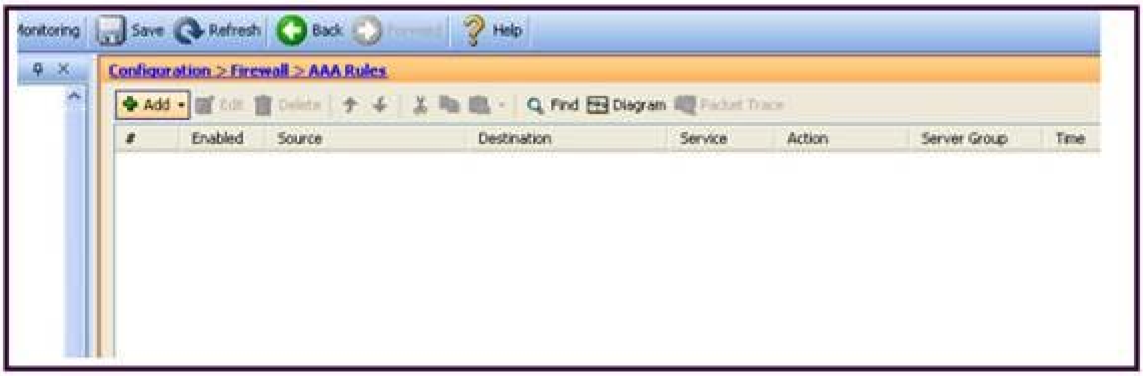
Question: 2

By default, which traffic can pass through a Cisco ASA that is operating in transparent mode without explicitly allowing it using an ACL?

A. ARP
B. BPDU
C. CDP
D. OSPF multicasts
E. DHCP

Answer: A

Question: 3

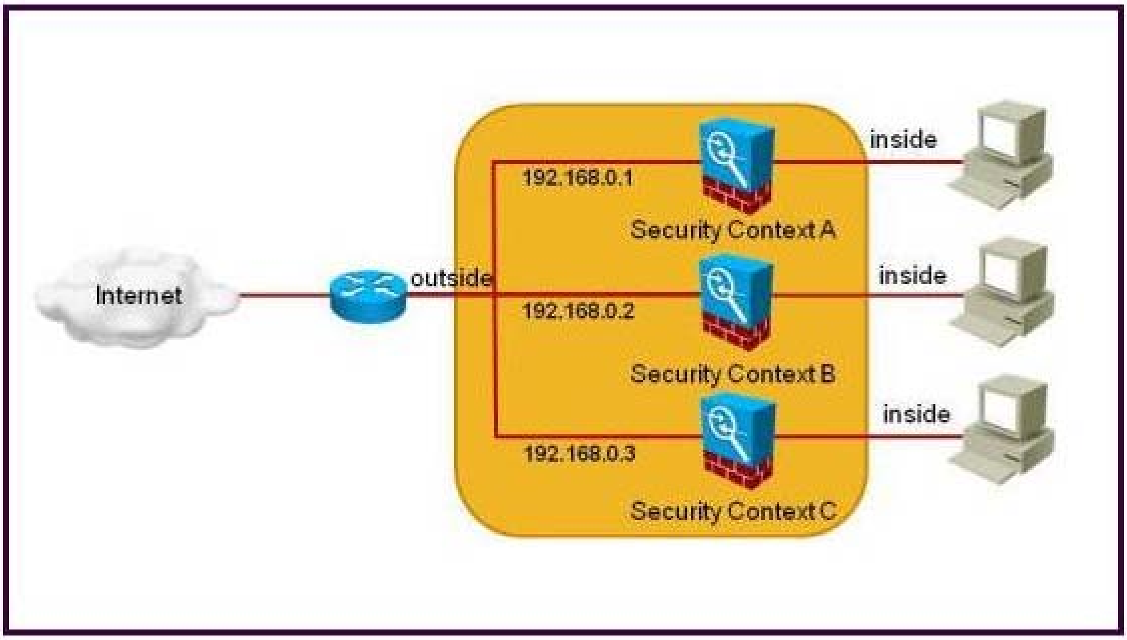


Referto the exhibit. Which Cisco ASA feature can be configured using this Cisco ASDM screen?

A. Cisco ASA command authorization using TACACS+
B. AAA accounting to track serial, ssh, and telnet connections to the Cisco ASA
C. Exec Shell access authorization using AAA
D. cut-thru proxy
E. AAA authentication policy for Cisco ASDM access

Answer: D

Question: 4



Refer to the exhibit. The Cisco ASA is dropping all the traffic that is sourced from the internet and is destined to any security context inside interface. Which configuration should be verified on the Cisco ASA to solve this problem?

A. The Cisco ASA has NAT control disabled on each security context.
B. The Cisco ASA is using inside dynamic NAT on each security context.
C. The Cisco ASA is using a unique MAC address on each security context outside interface.
D. The Cisco ASA is using a unique dynamic routing protocol process on each security context.
E. The Cisco ASA packet classifier is configured to use the outside physical interface to assign the packets to each security context.

Answer: C

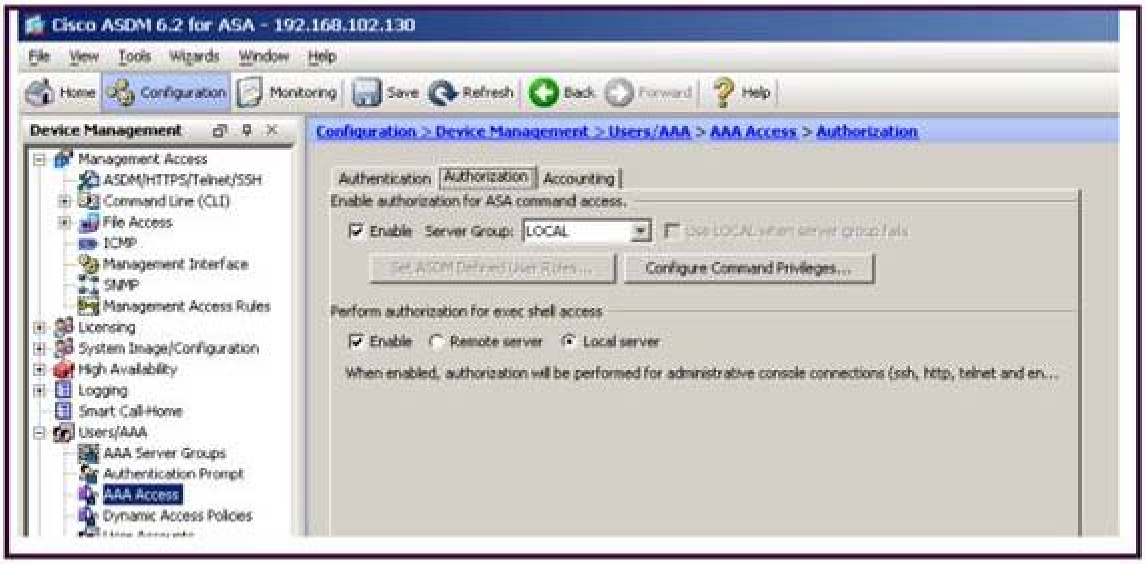
Question: 5

Which four types of ACL object group are supported on the Cisco ASA (release 8.2)? (Choose four.)

A. protocol
B. network
C. port
D. service
E. icmp-type
F. host

Answer: A,B,D,E

Question: 6



Configuration > Device Management > Users/AAA > AAA Access > Authorization

Enable authorization for ASA command access.

☑ Enable Server Group: LOCAL □ Use LOCAL when server group fails

Perform authorization for exec shell access

☑ Enable ○ Remote server ● Local server

When enabled, authorization will be performed for administrative console connections (ssh, http, telnet and en...

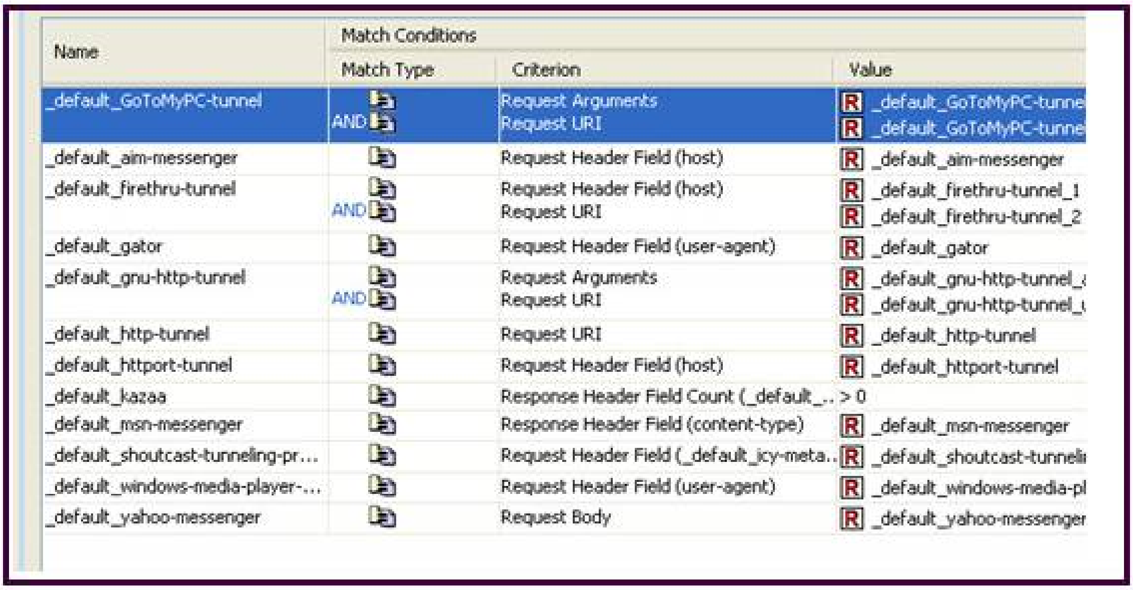
Refer to the exhibit. Which two CLI commands will result? (Choose two.)

A. aaa authorization network LOCAL
B. aaa authorization network default authentication-server LOCAL
C. aaa authorization command LOCAL
D. aaa authorization exec LOCAL
E. aaa authorization exec authentication-server LOCAL
F. aaa authorization exec authentication-server

Answer: C,D

Question: 7

Refer to the exhibit.



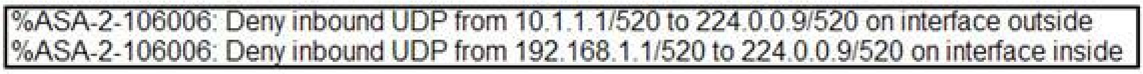
Name	Match Conditions		
	Match Type	Criterion	Value
_default_GoToMyPC-tunnel	 AND	Request Arguments Request URI	R _default_GoToMyPC-tunne R _default_GoToMyPC-tunne
_default_aim-messenger		Request Header Field (host)	R _default_aim-messenger
_default_firethru-tunnel	 AND	Request Header Field (host) Request URI	R _default_firethru-tunnel_1 R _default_firethru-tunnel_2
_default_gator		Request Header Field (user-agent)	R _default_gator
_default_gnu-http-tunnel	 AND	Request Arguments Request URI	R _default_gnu-http-tunnel_ R _default_gnu-http-tunnel_
_default_http-tunnel		Request URI	R _default_http-tunnel
_default_httport-tunnel		Request Header Field (host)	R _default_httport-tunnel
_default_kazaa		Response Header Field Count (_default_...	> 0
_default_msn-messenger		Response Header Field (content-type)	R _default_msn-messenger
_default_shoutcast-tunneling-pr...		Request Header Field (_default_icy-meta...	R _default_shoutcast-tunneli
_default_windows-media-player-...		Request Header Field (user-agent)	R _default_windows-media-pl
_default_yahoo-messenger		Request Body	R _default_yahoo-messenger

Which two statements about the class maps are true? (Choose two.)

A. These class maps are referenced within the global policy by default for HTTP inspection.
B. These class maps are all type inspect http class maps.
C. These class maps classify traffic using regular expressions.
D. These class maps are Layer 3/4 class maps.
E. These class maps are used within the inspection_default class map for matching the default inspection traffic.

Answer: B,E

Question: 8



```
%ASA-2-106006: Deny inbound UDP from 10.1.1.1/520 to 224.0.0.9/520 on interface outside
%ASA-2-106006: Deny inbound UDP from 192.168.1.1/520 to 224.0.0.9/520 on interface inside
```

Refer to the exhibit. A Cisco ASA in transparent firewall mode generates the log messages seen in the exhibit. What should be configured on the Cisco ASA to allow the denied traffic?

A. extended ACL on the outside and inside interface to permit the multicast traffic
B. EtherType ACL on the outside and inside interface to permit the multicast traffic
C. stateful packet inspection
D. static ARP mapping
E. static MAC address mapping

Answer: A