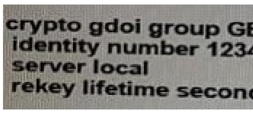
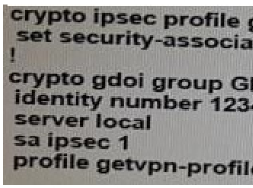
[Free-Dumps 400-251 New Questions and Answers -- Everybody Needs To Download For 100% Passing Exam (Question 181 &ndash; Question 210)

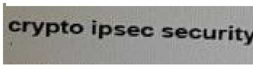
New Updated 400-251 Exam Questions from PassLeader 400-251 PDF dumps! Welcome to download the newest PassLeader 400-251 VCE dumps: http://www.passleader.com/400-251.html (366 Q&As) Keywords: 400-251 exam dumps, 400-251 exam questions, 400-251 VCE dumps, 400-251 PDF dumps, 400-251 practice tests, 400-251 study guide, 400-251 braindumps, CCIE Security Exam p.s. Free 400-251 dumps download from Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpd3JLalNVS0VWbms QUESTION 181What are two advantages of NBAR2 over NBAR? (Choose two.) A.   Only NBAR2 support Flexible NetFlow for extracting and exporting fields from the packet header.B.   Only NBAR2 allows the administrator to apply individual PDL files.C.   Only NBAR2 support PDLM to support new protocals.D.   Only NBAR2 can use Sampled NetFlow to extract pre-defined packet headers for reporting.E.   Only NBAR2 supports custom protocols based on HTTP URLs. Answer: AE QUESTION 182Which two statements about Network Edge Authentication Technology (NEAT) are true? (Choose two.) A.   It requires a standard ACL on the switch portB.   It conflicts with auto-configurationC.   It allows you to configure redundant links between authenticator and supplicant switchesD.   It supports port-based authentication on the authenticator switchE.   It can be configured on both access ports and trunk portsF.   It can be configured on both access ports and EtherChannel ports Answer: DE QUESTION 183What are three pieces of data you should review in response to a suspected SSL MITM attack? (Choose three.) A.   The IP address of the SSL serverB.   The X.509 certificate of the SSL serverC.   The MAC address of the attackerD.   The MAC address of the SSL serverE.   The X.509 certificate of the attackerF.   The DNS name off the SSL server Answer: ABF QUESTION 184From what type of server can you to transfer files to ASA's internal memory? A.   SSHB.   SFTPC.   NetlogonD.   SMB Answer: D QUESTION 185Which configuration is the correct way to change VPN key Encryption key lifetime to 10800 seconds on the key server?

A.


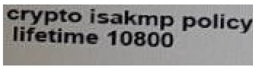
```
crypto gdoi group GE
 identity number 1234
 server local
 rekey lifetime secon
```

B.


```
crypto ipsec profile g
 set security-associa
!
crypto gdoi group GI
 identity number 123
 server local
 sa ipsec 1
 profile getvpn-profil
```

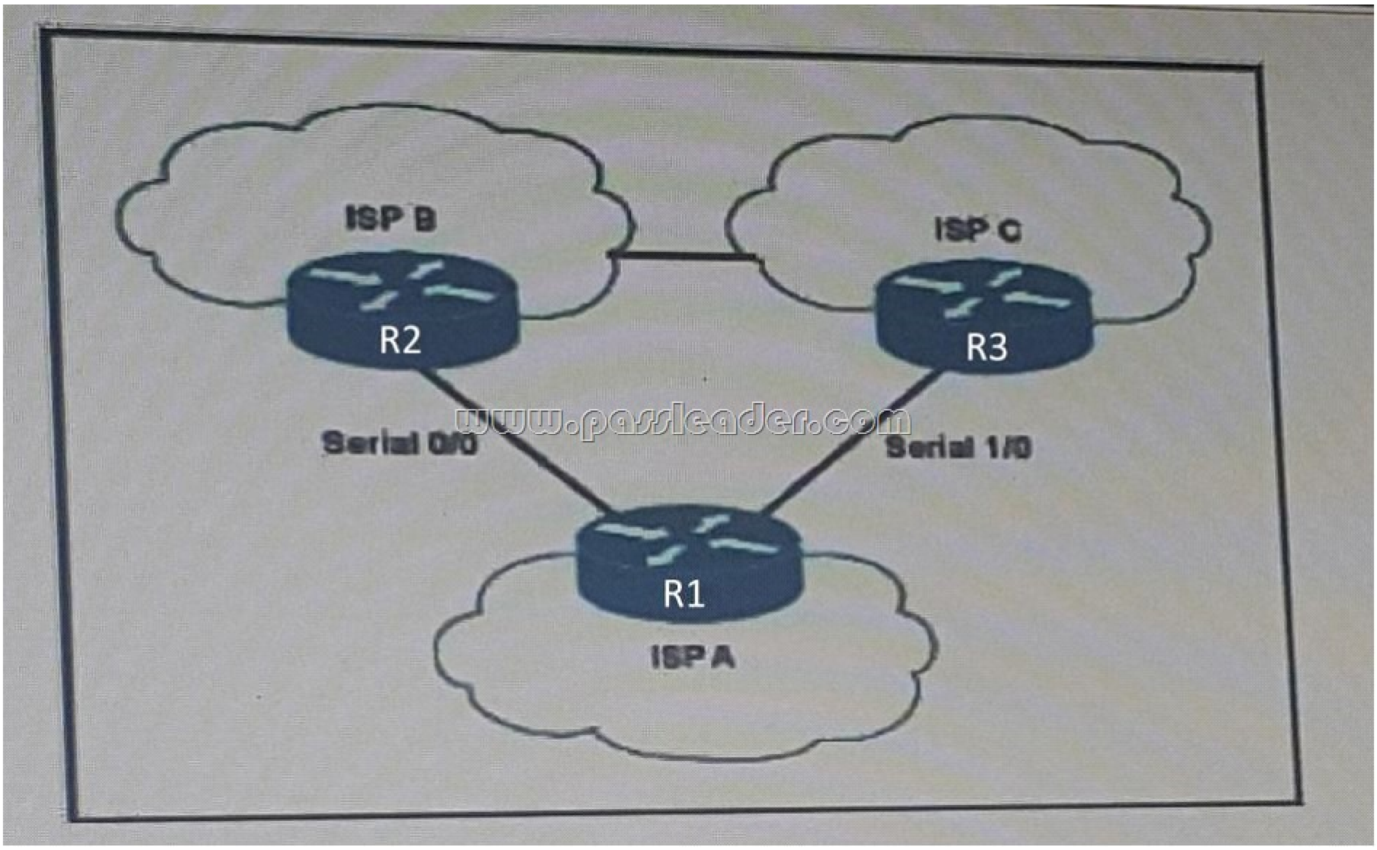
C.


```
crypto ipsec security
```

D.


```
crypto isakmp policy
 lifetime 10800
```

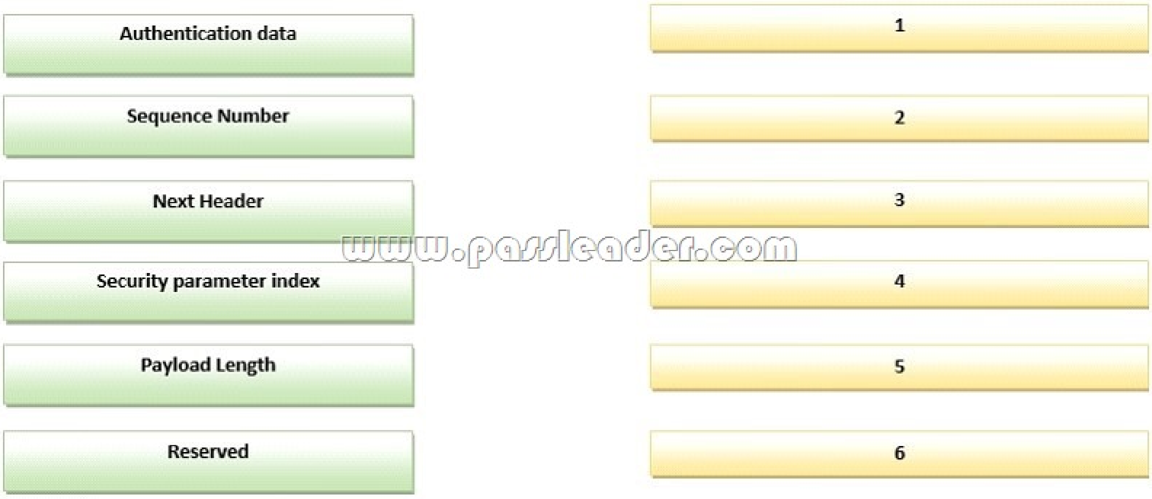
Answer: A QUESTION 186Which feature can you implement to protect against SYN-flooding DoS attacks? A.   the ip verify unicast reverse-path commandB.   a null zero routeC.   CAR applied to icmp packetsD.   TCP Intercept Answer: B QUESTION 187Refer to the exhibit. If R1 is connected upstream to R2 and R3 at different ISPs as shown, what action must be taken to prevent Unicast Reverse Path Forwarding (uRPF) from dropping asymmetric traffic?



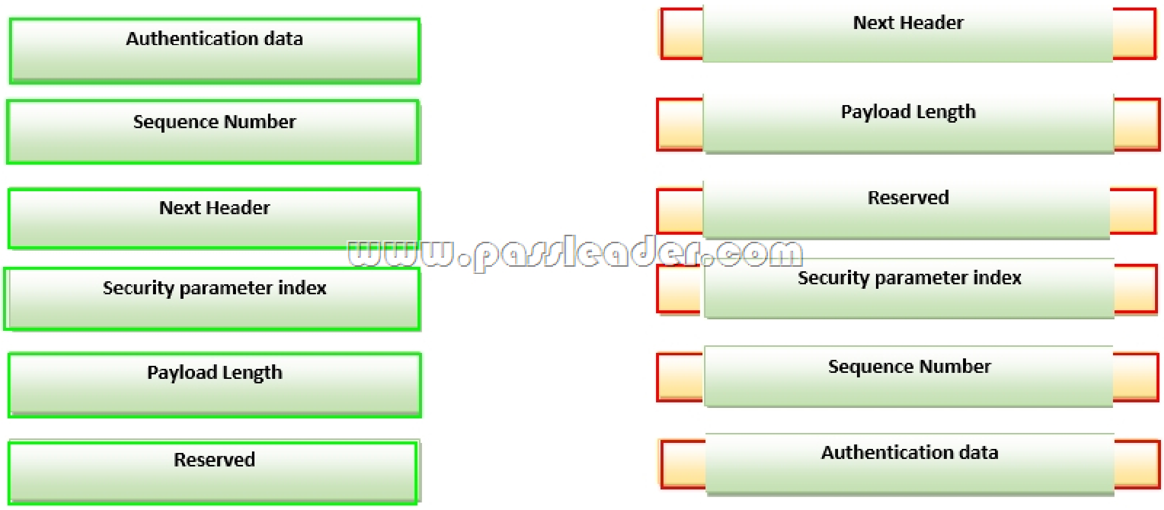
A. Configure Unicast RPF Loose Mode on R2 and R3 only.B. Configure Unicast RPF Loose Mode on R1 only.C. Configure Unicast RPF Strict Mode on R1 only.D. Configure Unicast RPF Strict Mode on R1,R2 and R3.E. Configure Unicast RPF Strict Mode on R2 and R3 only. Answer: E QUESTION 188Refer to the exhibit. Which effect of this Cisco ASA policy map is true?

```
policy-map
    paramete
        allow
```

A. The Cisco ASA is unable to examine the TLS session.B. The server ends the SMTP session with a QUIT command if the algorithm or key length is insufficiently secure.C. it prevents a STARTTLS session from being established.D. The Cisco ASA logs SMTP sessions in clear text. Answer: B QUESTION 189What security element must an organization have in place before it can implement a security audit and validate the audit results? A. firewallB. network access controlC. an incident response teamD. a security policyE. a security operation center Answer: D QUESTION 190Which two statements about RFC 2827 are true? (Choose two.) A. RFC 2827 defines egress packet filtering to safeguard against IP spoofing.B. A corresponding practice is documented by the IEFT in BCP 38.C. RFC 2827 defines ingress packet filtering for the multihomed network.D. RFC 2827 defines ingress packet filtering to defeat DoS using IP spoofing.E. A corresponding practice is documented by the IEFT in BCP 84. Answer: BD QUESTION 191From the list below, which one is the major benefit of AMP Threat GRID? A. AMP Threat Grid collects file information from customer servers and run tests on them to see if they are infected with virusesB. AMP Threat Grid learns ONLY from data you pass on your network and not from anything else to monitor for suspicious behavior. This makes the system much faster and efficientC. AMP Threat Grid combines Static, and Dynamic Malware analysis with threat intelligence into one combined solutionD. AMP Threat Grid analyzes suspicious behavior in your network against exactly 400 behavioral indicators Answer: C QUESTION 192Drag and Drop QuestionDrag each field authentication Header on the left into the order in which it appears in the header on the right.

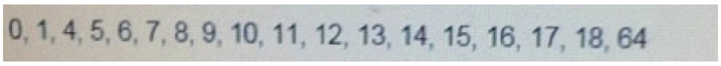


Answer:

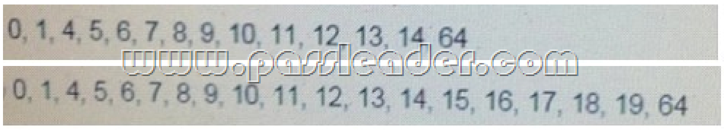


QUESTION 193Which two statement about Infrastructure ACLs on Cisco IOS software are true? (Choose two.) A. Infrastructure ACLs are used to block-permit the traffic in the router forwarding path.B. Infrastructure ACLs are used to block-permit the traffic handled by the route processor.C. Infrastructure ACLs are used to block-permit the transit traffic.D. Infrastructure ACLs only protect device physical management interface. Answer: BD QUESTION 194Which three statements about SCEP are true? (Choose three.) A. It Supports online certification revocation.B. Cryptographically signed and encrypted message are conveyed using PKCS#7.C. The certificate request format uses PKCS#10.D. It supports multiple cryptographic algorithms, including RSA.E. CRL retrieval is support through CDP (Certificate Distribution Point) queries.F. It supports Synchronous granting. Answer: BCE QUESTION 195class-map nbar_rtpmatch protocol rtp payload-type "0, 1, 4 - 0x10, 10001b - 10010b, 64"The above NBAR configuration matches RTP traffic with which payload types?

A.


0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 64

B.


0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 64

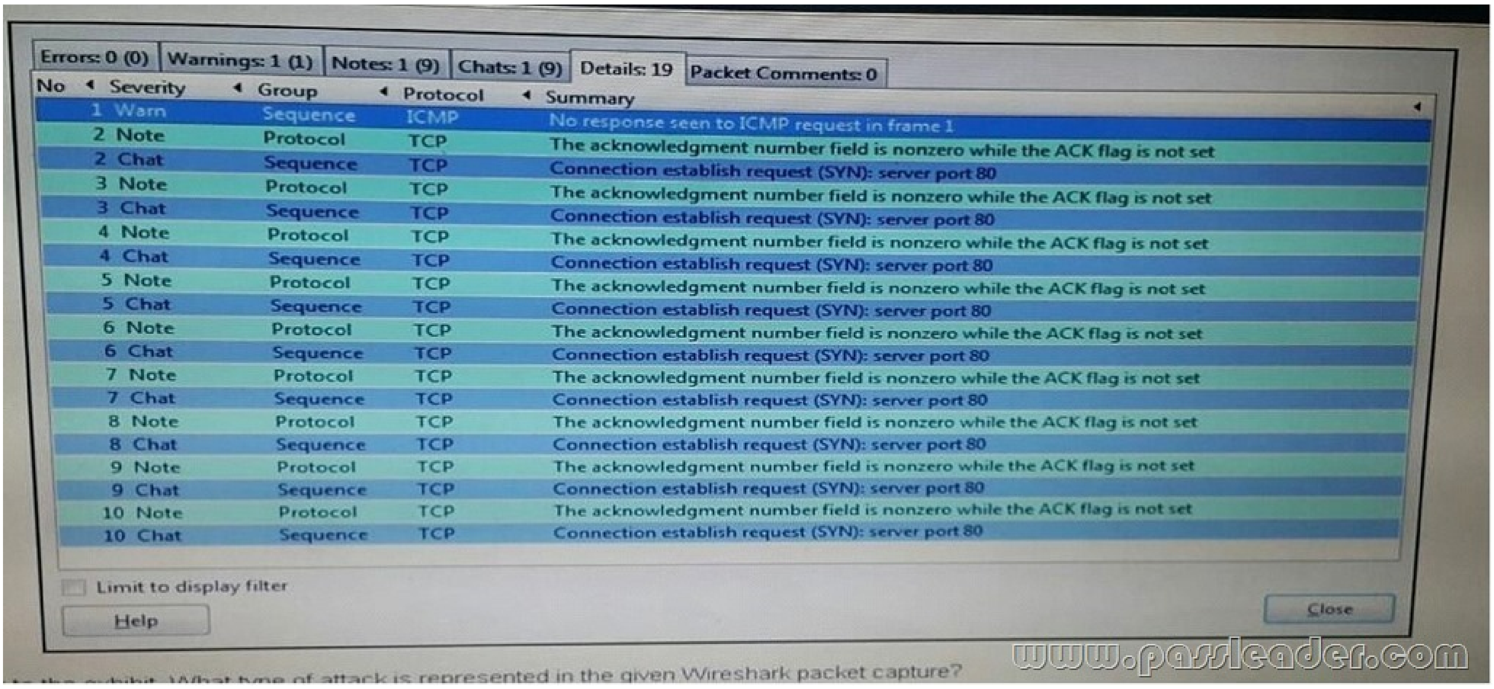
C.

0, 1, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 64

D.

0, 1, 4, 5, 6, 7, 8, 9, 10

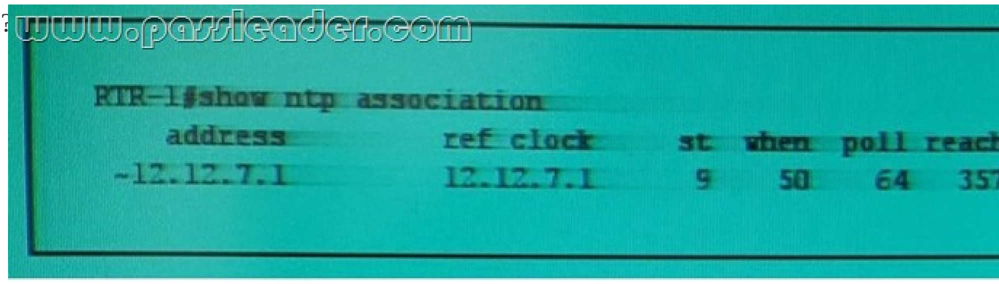
Answer: A QUESTION 196Refer to the exhibit. What type of attack is represented in the given Wireshark packet capture?



No	Severity	Group	Protocol	Summary
1	Warn	Sequence	ICMP	No response seen to ICMP request in frame 1
2	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
2	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
3	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
3	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
4	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
4	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
5	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
5	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
6	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
6	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
7	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
7	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
8	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
8	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
9	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
9	Chat	Sequence	TCP	Connection establish request (SYN): server port 80
10	Note	Protocol	TCP	The acknowledgment number field is nonzero while the ACK flag is not set
10	Chat	Sequence	TCP	Connection establish request (SYN): server port 80

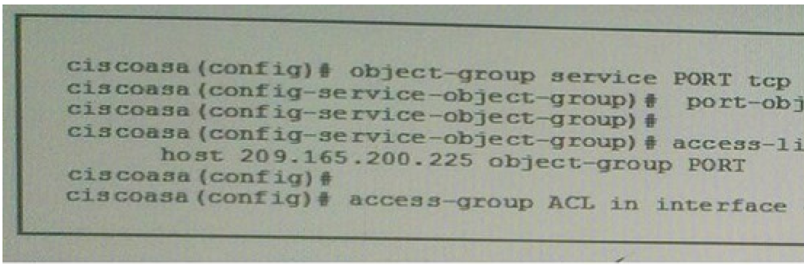
...the exhibit. What type of attack is represented in the given Wireshark packet capture?

A. a SYN floodB. spoofingC. a duplicate ACKD. TCP congestion controlE. a shrew attack Answer: A QUESTION 197 What message does the TACACS+ daemon send during the AAA authentication process to request additional authentication information? A. ACCEPTB. REJECTC. CONTINUED. ERRORE. REPLY Answer: C QUESTION 198Refer to the exhibit.While troubleshooting a router issue, you executed the show ntp association command and it returned this output. Which condition is indicated by the reach value of 357?



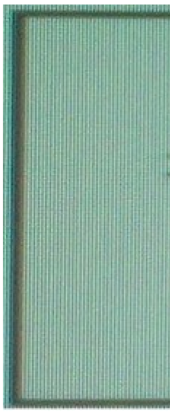
```
RTR-1#show ntp association
      address           ref clock      st  when  poll reach
  ~12.12.7.1            12.12.7.1       9    50    64   357
```

A. The NTP continuously received the previous 8 packets.B. The NTP process is waiting to receive its first acknowledgement. C. The NTP process failed to receive the most recent packet, but it received the 4 packets before the most recent packet.D. The NTP process received only the most recent packet. Answer: C QUESTION 199Which three IP resources is IANA responsible for? (Choose three.) A. IP address allocationB. detection of spoofed addressC. criminal prosecution of hackersD. autonomous system number allocationE. root zone management in DNSF. BGP protocol vulnerabilities Answer: ADE QUESTION 200 Which three attributes may be configured as part of the Common Tasks panel of an authorization profile in the Cisco ISE solution? (Choose three.) A. VLANB. voice VLANC. dACL nameD. voice domain permissionE. SGT Answer: ACD QUESTION 201Which two statements about DTLS are true? (Choose two.) A. It uses two simultaneous IPSec tunnels to carry traffic.B. If DPD is enabled, DTLS can fall back to a TLS connection.C. Because it requires two tunnels, it may experience more latency issues than SSL connections.D. If DTLS is disabled on an interface, then SSL VPN connections must use SSL/TLS tunnels.E. It is disabled by default if you enable SSL VPN on the interface. Answer: BC QUESTION 202Refer to the exhibit, which two Statements about the given Configuration are true? (Choose two.)

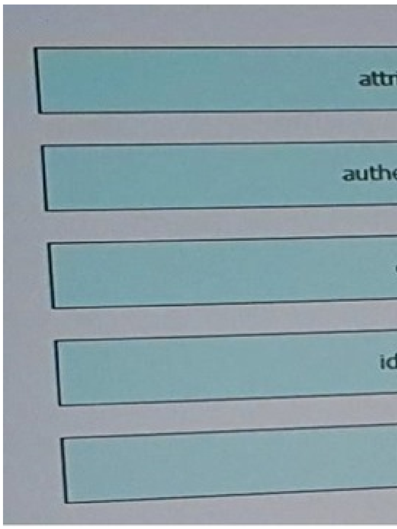


```
ciscoasa(config)# object-group service PORT tcp
ciscoasa(config-service-object-group)#  port-obj
ciscoasa(config-service-object-group)#
ciscoasa(config-service-object-group)# access-li
    host 209.165.200.225 object-group PORT
ciscoasa(config)#
ciscoasa(config)# access-group ACL in interface
```

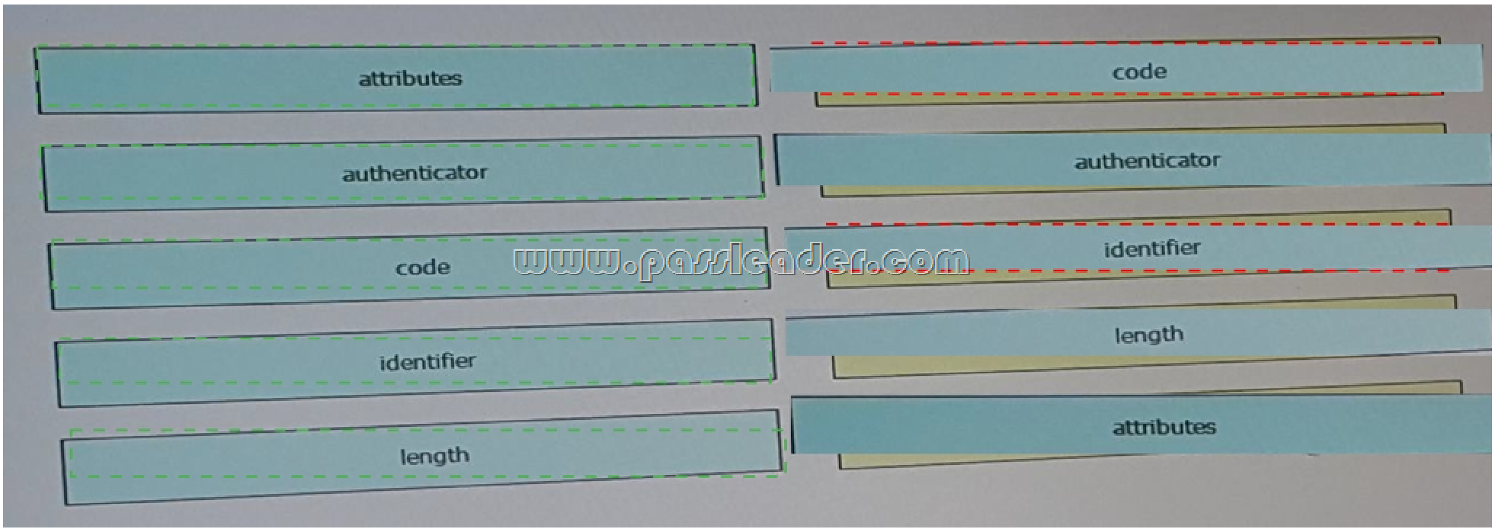
A. It is an inbound policy.B. It will allow 209.165.202.129 to connect to 202.165.200.225 on an IMAP port.C. It will allow 209.165.202.129 to connect to 202.165.200.225 on an RDP port.D. It will allow 202.165.200.225 to connect to 209.165.202.129 on an RDP port.E. It will allow 202.165.200.225 to connect to 209.165.202.129 on a VNC port.F. It is an outbound policy. Answer: AC QUESTION 203What command can you use to protect a router from TCP SYN-flooding attacks? A. ip igmp snoopingB. rate-limit input <bps><burst-normal><Burst-max>C. ip tcp intercept list <access-list>D. ip dns spoofing <ip-address>E. police <bps> Answer: C QUESTION 204Refer to the exhibit, what is the effect of the given configuration?



A. It will Drop all TTL packet with a value of 14 in the IP header field.B. It will Drop all TTL packet with a TTL value less than 14.C. It will Drop all TTL packet with a TTL value of 15 or more.D. It will Drop all TTL packet with a TTL value of 14 or more. Answer: B QUESTION 205If the ASA interfaces on a device are configured in passive mode, which mode must be configured on the remote device to enable EtherChannel? A. standbyB. activeC. onD. passive Answer: B QUESTION 206 Which three statements about the SHA-2 algorithm are true? (Choose three.) A. It provides a variable-length output using a collision-resistant cryptographic hash.B. It provides a fixed-length output using a collision-resistant cryptographic hash.C. It is used for integrity verification.D. It generates a 160-bit message digest.E. It is the collective term for the SHA-224, SHA-256, SHA-384, and SHA-512 algorithms.F. It generates a 512-bit message digest. Answer: BCE QUESTION 207Drag and Drop QuestionDrag and drop each RADIUS packet field on the left onto the matching decription on the right.



Answer:



QUESTION 208Which three of these situation warrant engagement of a security incident Response team? (Choose three.) A. damage to computer/network resourcesB. pornographic biogs'websitesC. computer or network misuse/abuseD. denial of service (DoS)E. loss of data confidentialitymtegrity Answer: CDE QUESTION 209What are three protocol that support layer 7 class maps and policy maps for zone based firewalls? (Choose three.) A. IMAPB. RDPC. MMED. ICQE. POP3F. IKE Answer: ADE QUESTION 210You have configured an authenticator switch in access mode on a network configured with NEAT what radius attribute must the ISE server return to change the switch's port mode to trunk? A. device-traffic-class=switchB. device-traffic-class=trunkC. framed-protocol=1D. EAP-message-switchE. Authenticate=AdministrativeF. Acct-Authentic=radius Answer: A Download the newest PassLeader 400-251 dumps from passleader.com now! 100% Pass Guarantee! 400-251 PDF dumps & 400-251 VCE dumps: http://www.passleader.com/400-251.html (366 Q&As) (New Questions Are 100% Available and Wrong Answers Have Been Corrected! Free VCE simulator!) p.s. Free 400-251 dumps download from Google Drive: https://drive.google.com/open?id=0B-ob6L_QjGLpd3JLalNVS0VWbms