[Feb-2019Valid 300-206 PDF Dumps and 300-206 VCE Free Download in Braindump2go(Q170-Q180)

2019/Feb Braindump2go 300-206 Exam Dumps with PDF and VCE New Updated Today! Following are some new 300-206 Real Exam Questions:1.|2019 Latest 300-206 Exam Dumps (VCE & PDF)
Download:https://www.braindump2go.com/300-206.html2.|2019 Latest 300-206 Exam Questions & Answers
Download:https://drive.google.com/drive/folders/0B75b5xYLjSSNOXZTcmdGNEh2UU0?usp=sharingQUESTION 170Which kind of Layer 2 attack targets the STP root bridge election process and allows an attacker to control the flow of traffic?A. man-in-the-middleB. denial of serviceC. distributed denial of serviceD. CAM overflow**Answer: A**QUESTION 171Which Layer 2 security feature validates ARP packets?A. DAIB. DHCP serverC. BPDU guardD. BPDU filtering**Answer: A** QUESTION 172If you disable PortFast on switch ports that are connected to a Cisco ASA and globally turn on BPDU filtering, what is the effect on the switch ports?A. The switch ports are prevented from going into an err-disable state if a BPDU is received. B. The switch ports are prevented from going into an err-disable state if a BPDU is sent.C. The switch ports are prevented from going into an err-disable state if a BPDU is received and sent.D. The switch ports are prevented from forming a trunk.**Answer: C** QUESTION 173In a Cisco ASAv failover deployment, which interface is preconfigured as the failover interface?A. GigabitEthernet0/2B. GigabitEthernet0/4C. GigabitEthernet0/6D. GigabitEthernet0/8**Answer: D**QUESTION 174What are the three types of private VLAN ports? (Choose three.)A. promiscuousB. isolatedC. communityD. primaryE. secondaryF. trunk**Answer: ABC**QUESTION 175Which VTP mode supports private VLANs on a switch?A. transparentB. serverC. client D. off**Answer: A**QUESTION 176Which technology can be deployed with a Cisco ASA 1000V to segregate Layer 2 access within a virtual cloud environment?A. Cisco Nexus 1000VB. Cisco VSGC. WSVAD. ESVA**Answer: A**QUESTION 177Which cloud characteristic is used to describes the sharing of physical resources between various entities ?A. ElasticityB. Ubiquitous accessC. MultitenancyD. ResiliencyAnswer: CExplanation:Resource pooling/Multi-Tenancy: The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state or datacenter). Examples of resources include storage, processing, memory and network bandwidth.QUESTION 178Refer to the exhibit. Which type of ACL is shown in this configuration? A. IPv4B. IPv6C. unifiedD. IDFW**Answer: C**QUESTION 179You are the network security engineer for the Secure-X network. The company has recently detected Increase of traffic to malware Infected destinations. The Chief Security Officer deduced that some PCs in the internal networks are infected with malware and communicate with malware infected destinations.The CSO has tasked you with enable Botnet traffic filter on the Cisco ASA to detect and deny further connection attempts from infected PCs to malware destinations. You are also required to test your configurations by initiating connections through the Cisco ASA and then display and observe the Real-Time Log Viewer in ASDM.To successfully complete this activity, you must perform the following tasks:- Download the dynamic database and enable use of it.- Enable the ASA to download of the dynamic database- Enable the ASA to download of the dynamic database.- Enable DNS snooping for existing DNS inspection service policy rules..- Enable Botnet Traffic Filter classification on the outside interface for All Traffic.- Configure the Botnet Traffic Filter to drop blacklisted traffic on the outside interface. Use the default Threat Level settingsNOTE: The database files are stored in running memory; they are not stored in flash memory.NOTE: DNS is enabled on the inside interface and set to the HQ-SRV (10.10.3.20).NOTE: Not all ASDM screens are active for this exercise.- Verify that the ASA indeed drops traffic to blacklisted destinations by doing the following:- From the Employee PC, navigate to **http://www.google.com** to make sure that access to the Internet is working.- From the Employee PC, navigate to **http://bot-sparta.no-ip.org**. This destination is classified as malware destination by the Cisco SIO database.- From the Employee PC, navigate to **http://superzarabotok-gid.ru/**. This destination is classified as malware destination by the Cisco SIO database.- From Admin PC, launch ASDM to display and observe the Real-Time Log Viewer.You have completed this exercise when you have configured and successfully tested Botnet traffic filter on the Cisco ASA.See the explanation for detailed answer to this sim question.First, click on both boxes on the Botnet Database as shown below and hit apply:Click Yes to send the commands when prompted.Then, click on the box on the DNS Snooping page as shown below and hit apply:Click Yes to send the commands when prompted.Then, click on the box on the Traffic Settings tab as shown:At which point this pop-up box will appear when you click on the Add button:Click OK. Then Apply. Then Send when prompted.Then verify that all is working according to the instructions given in the question.QUESTION 180You are a network security engineer for the Secure-X network. You have been tasked with implementing dynamic network object NAT with PAT on a Cisco ASA. You must configure the Cisco ASA such that

the source IP addresses of all internal hosts are translated to a single IP address (using different ports) when the internal hosts access the Internet.To successfully complete this activity, you must perform the following tasks:- Use the Cisco ASDM GUI on the Admin PC to configure dynamic network object NAT with PAT using the following parameters:- Network object name: Internal-Networks- IP subnet: 10.10.0.0/16- Translated IP address: 192.0.2.100- Source interface: inside- Destination interface: outsideNOTE: The object (TRANSLATED-INSIDE-HOSTS) for this translated IP address has already been created for your use in this activity.NOTE: Not all ASDM screens are active for this exercise.NOTE: Login credentials are not needed for this simulation.- In the Cisco ASDM, display and view the auto-generated NAT rule.- From the Employee PC, generate traffic to SP-SRV by opening a browser and navigating to **http://sp-srv.sp.public**.- From the Guest PC, generate traffic to SP-SRV by opening a browser and navigating to **http://sp-srv.sp.public**.- At the CLI of the Cisco ASA, display your NAT configuration. You should see the configured policy and statistics for translated packets.- At the CLI of the Cisco ASA, display the translation table. You should see dynamic translations for the Employee PC and the Guest PC. Both inside IP addresses translate to the same IP address, but using different ports.You have completed this exercise when you have configured and successfully tested dynamic network object NAT with PAT.Answer: See the explanation for detailed answer to this sim question.First, click on Add Network Objects on the Network Objects/Groups tab and fill in the information as shown below:Then, use the advanced tab and configure it as shown below:Then hit OK, OK again, Apply, and then Send when prompted. You can verify using the instructions provided in the question!!!RECOMMEND!!!1.|2019 Latest 300-206 Exam Dumps (VCE & PDF) Download:https://www.braindump2go.com/300-206.html2.|2019 Latest 300-206 Study Guide Video: YouTube Video: YouTube.com/watch?v=o-P9VZB3MsE