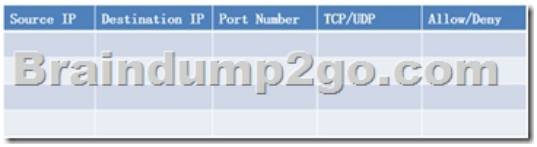
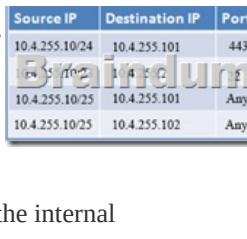
[Aug.-2016-NEWBraindump2go CompTIA 1867Q&As SY0-401 Exam PDF & VCE [NQ11-NQ20 Share

2016/08 SY0-401: CompTIA Security+ Certification Exam Questions New Updated Today! Free Instant Download SY0-401 Exam Dumps(PDF & VCE) 1867Q&As from Braindump2go.com!100% Real Exam Questions! 100% Exam Pass Guaranteed! NEW QUESTION 11 - NEW QUESTION 20: 1.|2016/08 SY0-401 Exam Dumps(PDF & VCE) 1867Q&As Download:http://www.braindump2go.com/sy0-401.html 2.|2016/08 SY0-401 Exam Questions & Answers:https://drive.google.com/folderview?id=0B75b5xYLjSSNTldvc1ZkQlNUc0k&usp=sharing QUESTION 11An administrator would like to review the effectiveness of existing security in the enterprise. Which of the following would be the BEST place to start? A. Review past security incidents and their resolutionB. Rewrite the existing security policyC. Implement an intrusion prevention systemD. Install honey pot systems Answer: CExplanation:The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it QUESTION 12A company has proprietary mission critical devices connected to their network which are configured remotely by both employees and approved customers. The administrator wants to monitor device security without changing their baseline configuration. Which of the following should be implemented to secure the devices without risking availability? A. Host-based firewallB. IDSC. IPSD. Honeypot Answer: BExplanation:An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. IDS come in a variety of "flavors" and approach the goal of detecting suspicious traffic in different ways. There are network based (NIDS) and host based (HIDS) intrusion detection systems. Some systems may attempt to stop an intrusion attempt but this is neither required nor expected of a monitoring system. Intrusion detection and prevention systems (IDPS) are primarily focused on identifying possible incidents, logging information about them, and reporting attempts. In addition, organizations use IDPSes for other purposes, such as identifying problems with security policies, documenting existing threats and deterring individuals from violating security policies. IDPSes have become a necessary addition to the security infrastructure of nearly every organization.IDPSes typically record information related to observed events, notify security administrators of important observed events and produce reports. Many IDPSes can also respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques, which involve the IDPS stopping the attack itself, changing the security environment (e.g. reconfiguring a firewall) or changing the attack's content. QUESTION 13Lab Sim - Configure the FirewallTask: Configure the firewall (fill out the table) to allow these four rules:- Only allow the Accounting computer to have HTTPS access to the Administrative server.- Only allow the HR computer to be able to communicate with the Server 2 System over SCP.- Allow the IT computer to have access to both the Administrative Server 1 and Administrative Server 2

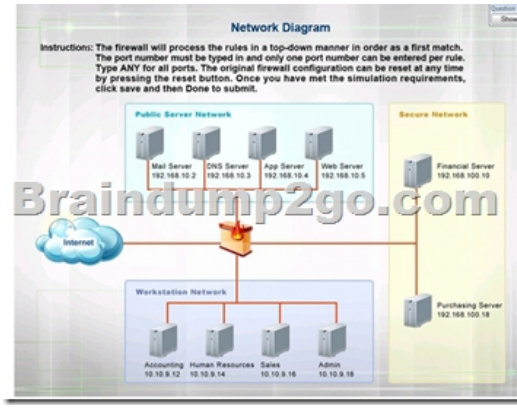


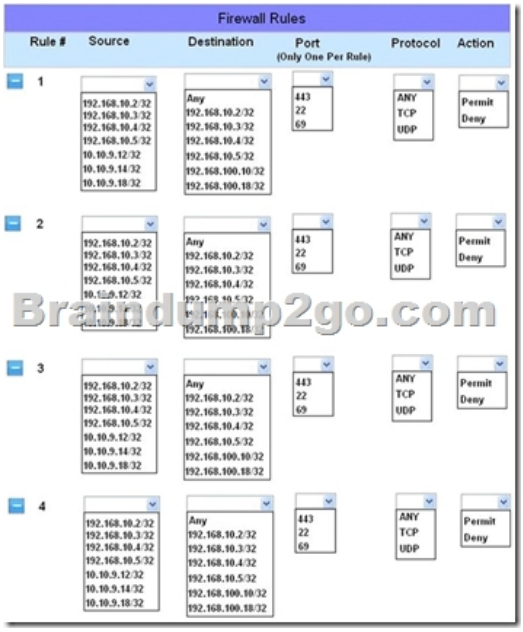
Answer: Use the following answer for this simulation task. Below table has all the answers required for this question.



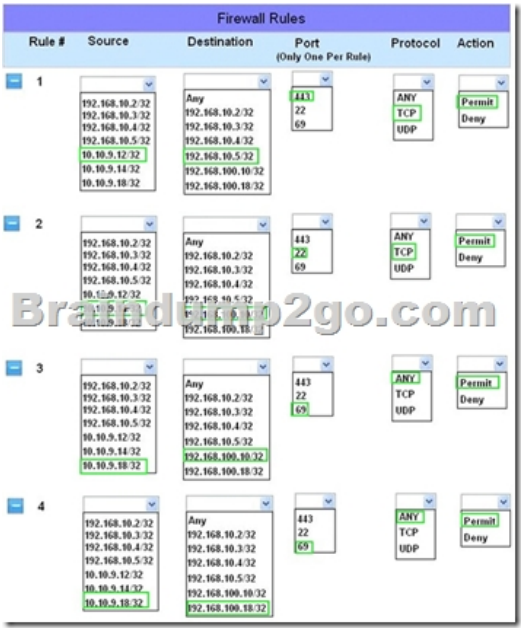
Explanation:Firewall rules act like ACLs, and they are used to dictate what traffic can pass between the firewall and the internal network. Three possible actions can be taken based on the rule's criteria:Block the connectionAllow the connectionAllow the connection only if it is securedTCP is responsible for providing a reliable, one-to-one, connection-oriented session. TCP establishes a connection and ensures that the other end receives any packets sent. Two hosts communicate packet results with each other. TCP also ensures that packets are decoded and sequenced properly. This connection is persistent during the session. When the session ends, the connection is torn down.UDP provides an unreliable connectionless communication method between hosts. UDP is considered a best-effort protocol, but it's considerably faster than TCP. The sessions don't establish a synchronized session like the kind used in TCP, and UDP doesn't guarantee error-free communications. The primary purpose of UDP is to send small packets of information. The application is responsible for acknowledging the correct reception of the data.Port 22 is used by both SSH and SCP with UDP.Port 443 is used for secure web connections ?HTTPS and is a TCP port. Thus to make sure only the Accounting computer has HTTPS access to the Administrative server you should use TCP port 443 and set the rule to allow communication between

10.4.255.10/24 (Accounting) and 10.4.255.101 (Administrative server1) Thus to make sure that only the HR computer has access to Server2 over SCP you need use of TCP port 22 and set the rule to allow communication between 10.4.255.10/23 (HR) and 10.4.255.2 (server2)Thus to make sure that the IT computer can access both the Administrative servers you need to use a port and accompanying port number and set the rule to allow communication between:10.4.255.10.25 (IT computer) and 10.4.255.101 (Administrative server1)10.4.255.10.25 (IT computer) and 10.4.255.102 (Administrative server2) QUESTION 14Hotspot Question The security administrator has installed a new firewall which implements an implicit DENY policy by default Click on the firewall and configure it to allow ONLY the following communication.1. The Accounting workstation can ONLY access the web server on the public network over the default HTTPS port. The accounting workstation should not access other networks.2. The HR workstation should be restricted to communicate with the Financial server ONLY, over the default SCP port3. The Admin workstation should ONLY be able to access the servers on the secure network over the default TFTP port.Instructions: The firewall will process the rules in a top-down manner in order as a first match The port number must be typed in and only one port number can be entered per rule Type ANY for all ports. The original firewall configuration can be reset at any time by pressing the reset button. Once you have met the simulation requirements, click save and then Done to submit.





Answer:



Explanation:Implicit deny is the default security stance that says if you aren't specifically granted access or privileges for a resource, you're denied access by default.Rule #1 allows the Accounting workstation to ONLY access the web server on the public network over the default HTTPS port, which is TCP port 443.Rule #2 allows the HR workstation to ONLY communicate with the Financial server over the default SCP port, which is TCP Port 22Rule #3 & Rule #4 allow the Admin workstation to ONLY access the Financial and Purchasing servers located on the secure network over the default TFTP port, which is Port 69. QUESTION 15Which of the following firewall rules only denies DNS zone transfers? A. deny udp any any port 53B. deny ip any anyC. deny tcp any any port 53D. deny all dns packets Answer: CExplanation:DNS operates over TCP and UDP port 53. TCP port 53 is used for zone transfers. QUESTION 16A security administrator suspects that an increase in the amount of TFTP traffic on the network is due to unauthorized file transfers, and wants to configure a firewall to block all TFTP traffic.Which of the following would accomplish this task? A. Deny TCP port 68B. Deny TCP port 69C. Deny UDP port 68D. Deny UDP port 69 Answer: DExplanation:Trivial File Transfer Protocol (TFTP) is a simple file-exchange protocol that doesn't require authentication. It operates on UDP port 69. QUESTION 17Sara, a security technician, has received notice that a vendor coming in for a presentation will require access to a server outside of the network. Currently, users are only able to access remote sites through a VPN connection. How could Sara BEST accommodate the vendor? A. Allow incoming IPSec traffic into the vendor's IP address.B. Set up a VPN account for the vendor, allowing access to the remote site.C. Turn off the firewall while the vendor is in the office, allowing access to the remote site.D. Write a firewall rule to allow the vendor to have access to the remote site. Answer: DExplanation:Firewall rules are used to define what traffic is able pass between the firewall and the internal network. Firewall rules block the connection, allow the connection, or allow the connection only if it is secured. Firewall rules can be applied to inbound traffic or outbound traffic and any type of network. QUESTION 18A technician is deploying virtual machines for multiple customers on a single physical host to reduce power consumption in a data center. Which of the following should be recommended to isolate the VMs from one another? A. Implement a virtual firewallB. Install HIPS on each VMC. Virtual switches with VLANsD. Develop a patch management guide Answer: CExplanation:A virtual local area network (VLAN) is a hardware-imposed network segmentation created by switches. VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments. QUESTION 19 A router has a single Ethernet connection to a switch. In the router configuration, the Ethernet interface has three sub-interfaces, each configured with ACLs applied to them and 802.1q trunks.Which of the following is MOST likely the reason for the sub-interfaces? A. The network uses the subnet of 255.255.255.128.B. The switch has several VLANs configured on it.C. The sub-interfaces are configured for VoIP traffic.D. The sub-interfaces each implement quality of service. Answer: BExplanation:A subinterface is a division of one physical interface into multiple logical interfaces. Routers commonly employ subinterfaces for a variety of purposes, most common of these are for routing traffic between VLANs. Also, IEEE 802.1Q is the networking standard that supports virtual LANs (VLANs) on an Ethernet network. QUESTION 20Joe, a technician at the local power plant, notices that several turbines had ramp up in cycles during the week. Further investigation by the system engineering team determined that a timed .exe file had been uploaded to the system control console during a visit by international contractors. Which of the following

actions should Joe recommend? A. Create a VLAN for the SCADAB. Enable PKI for the MainFrameC. Implement patch managementD. Implement stronger WPA2 Wireless Answer: AExplanation:VLANs are used for traffic management. VLANs can be used to isolate traffic between network segments. This can be accomplished by not defining a route between different VLANs or by specifying a deny filter between certain VLANs (or certain members of a VLAN). Any network segment that doesn't need to communicate with another in order to accomplish a work task/function shouldn't be able to do so. !!!RECOMMEND!!! 1.|2016/08 SY0-401 PDF Dumps & VCE Dumps 1867Q&As Download: http://www.braindump2go.com/sy0-401.html 2.|2016/08 SY0-401 Questions & Answers: https://drive.google.com/folderview?id=0B75b5xYLjSSNTldvc1ZkQlNUc0k&usp=sharing