[January 2018 Lead2pass 300-101 Exam Dumps New Updated By Cisco Official Exam Center 489q

300-101 New Questions Free Download In Lead2pass: https://www.lead2pass.com/300-101.html QUESTION 1A network engineer has been asked to ensure that the PPPoE connection is established and authenticated using an encrypted password. Which technology, in combination with PPPoE, can be used for authentication in this manner? A. PAPB. dot1xC. IPsecD. CHAPE. ESPAnswer: DExplanation:With PPPoE, the two authentication options are PAP and CHAP. When CHAP is enabled on an interface and a remote device attempts to connect to it, the access server sends a CHAP packet to the remote device. The CHAP packet requests or "challenges" the remote device to respond. The challenge packet consists of an ID, a random number, and the host name of the local router. When the remote device receives the challenge packet, it concatenates the ID, the remote device's password, and the random number, and then encrypts all of it using the remote device's password. The remote device sends the results back to the access server, along with the name associated with the password used in the encryption process. When the access server receives the response, it uses the name it received to retrieve a password stored in its user database. The retrieved password should be the same password the remote device used in its encryption process. The access server then encrypts the concatenated information with the newly retrieved password--if the result matches the result sent in the response packet, authentication succeeds.The benefit of using CHAP authentication is that the remote device's password is never transmitted in clear text (encrypted). This prevents other devices from stealing it and gaining illegal access to the ISP's network. http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfathen.html QUESTION 2A corporate policy requires PPPoE to be enabled and to maintain a connection with the ISP, even if no interesting traffic exists. Which feature can be used to accomplish this task? A. TCP AdjustB. Dialer PersistentC. PPPoE GroupsD. half-bridgingE. Peer Neighbor Route Answer: BExplanation:A new interface configuration command, dialer persistent, allows a dial-on-demand routing (DDR) dialer profile connection to be brought up without being triggered by interesting traffic. When configured, the dialer persistent command starts a timer when the dialer interface starts up and starts the connection when the timer expires. If interesting traffic arrives before the timer expires, the connection is still brought up and set as persistent. The command provides a default timer interval, or you can set a custom timer interval. QUESTION 3Which encapsulation supports an interface that is configured for an EVN trunk? A. 802.1QB. ISLC. PPPD. Frame RelayE. MPLSF. HDLC Answer: AExplanation:Restrictions for EVNAn EVN trunk is allowed on any interface that supports 802.1q encapsulation, such as Fast Ethernet, Gigabit Ethernet, and port channels.A single IP infrastructure can be virtualized to provide up to 32 virtual networks end-to-end. If an EVN trunk is configured on an interface, you cannot configure VRF-Lite on the same interface.OSPFv3 is not supported; OSPFv2 is supported. http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/evn/configuration/xe-3s/evn-xe-3s-book/evn-overview.pdf QUESTION 4Which three characteristics are shared by subinterfaces and associated EVNs? (Choose three.) A. IP addressB. routing tableC. forwarding tableD. access control listsE. NetFlow configuration Answer: ABCExplanation:runk interface can carry traffic for multiple EVNs. To simplify the configuration process, all the subinterfaces and associated EVNs have the same IP address assigned. In other words, the trunk interface is identified by the same IP address in different EVN contexts. This is accomplished as a result of each EVN having a unique routing and forwarding table, thereby enabling support for overlapping IP addresses across multiple EVNs.http://www.cisco.com/en/US/docs/ios-xml/ios/evn/configuration/xe-3sg/evn-overview.pdf QUESTION 5Which traffic does the following configuration allow? ipv6 access-list ciscopermit ipv6 host 2001:DB8:0:4::32 any eq sshline vty 0 4ipv6 access-class cisco in A. all traffic to vty 0 4 from source 2001:DB8:0:4::32B. only ssh traffic to vty 0 4 from source allC. only ssh traffic to vty 0 4 from source 2001:DB8:0:4::32D. all traffic to vty 0 4 from source all Answer: CExplanation:Here we see that the Ipv6 access list called "cisco" is being applied to incoming VTY connections to the router. Ipv6 access list has just one entry, which allows only the single Ipv6 IP address of 2001:DB8:0:4::32 to connect using SSH only. QUESTION 6For troubleshooting purposes, which method can you use in combination with the debug ip packet command to limit the amount of output data? A. You can disable the IP route cache globally.B. You can use the KRON scheduler.C. You can use an extended access list.D. You can use an IOS parser.E. You can use the RITE traffic exporter. Answer: CExplanation:The "debug ip packet" command generates a substantial amount of output and uses a substantial amount of system resources. This command should be used with caution in production networks. Always use with the access-list command to apply an extended ACL to the debug output. http://www.cisco.com/c/en/us/support/docs/security/dynamic-multipoint-vpn-dmvpn/111976-dmvpn-troubleshoot-00.html QUESTION 7Refer to the following access list. access-list 100 permit ip any any log After applying the access list on a Cisco router, the network engineer notices that the router CPU utilization has risen to 99 percent. What is the reason for this? A. A packet that matches access-list with the "log" keyword is Cisco Express Forwarding switched.B. A packet that matches access-list with the

"log" keyword is fast switched.C. A packet that matches access-list with the "log" keyword is process switched.D. A large amount of IP traffic is being permitted on the router. Answer: CExplanation:ging-enabled access control lists (ACLs) provide insight into traffic as it traverses the network or is dropped by network devices. Unfortunately, ACL logging can be CPU intensive and can negatively affect other functions of the network device. There are two primary factors that contribute to the CPU load increase from ACL logging: process switching of packets that match log-enabled access control entries (ACEs) and the generation and transmission of log messages.http://www.cisco.com/web/about/security/intelligence/acl-logging.html#4 QUESTION 8Which address is used by the Unicast Reverse Path Forwarding protocol to validate a packet against the routing table? A. source addressB. destination addressC. router interfaceD. default gateway Answer: AExplanation:The Unicast RPF feature helps to mitigate problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network by discarding IP packets that lack a verifiable IP source address. For example, a number of common types of denial-of-service (DoS) attacks, including Smurf and Tribal Flood Network (TFN), can take advantage of forged or rapidly changing source IP addresses to allow attackers to thwart efforts to locate or filter the attacks. For Internet service providers (ISPs) that provide public access, Unicast RPF deflects such attacks by forwarding only packets that have source addresses that are valid and consistent with the IP routing table. This action protects the network of the ISP, its customer, and the rest of the Internet.
http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scfrpf.html QUESTION 9What are the three modes of Unicast Reverse Path Forwarding? A. strict mode, loose mode, and VRF modeB. strict mode, loose mode, and broadcast modeC. strict mode, broadcast mode, and VRF modeD. broadcast mode, loose mode, and VRF mode Answer: AExplanation:Network administrators can use Unicast Reverse Path Forwarding (Unicast RPF) to help limit the malicious traffic on an enterprise network. This security feature works by enabling a router to verify the reachability of the source address in packets being forwarded. This capability can limit the appearance of spoofed addresses on a network. If the source IP address is not valid, the packet is discarded. Unicast RPF works in one of three different modes: strict mode, loose mode, or VRF mode. Note that not all network devices support all three modes of operation. Unicast RPF in VRF mode will not be covered in this document.When administrators use Unicast RPF in strict mode, the packet must be received on the interface that the router would use to forward the return packet. Unicast RPF configured in strict mode may drop legitimate traffic that is received on an interface that was not the router's choice for sending return traffic. Dropping this legitimate traffic could occur when asymmetric routing paths are present in the network.When administrators use Unicast RPF in loose mode, the source address must appear in the routing table. Administrators can change this behavior using the allow-default option, which allows the use of the default route in the source verification process. Additionally, a packet that contains a source address for which the return route points to the Null 0 interface will be dropped. An access list may also be specified that permits or denies certain source addresses in Unicast RPF loose mode.Care must be taken to ensure that the appropriate Unicast RPF mode (loose or strict) is configured during the deployment of this feature because it can drop legitimate traffic. Although asymmetric traffic flows may be of concern when deploying this feature, Unicast RPF loose mode is a scalable option for networks that contain asymmetric routing paths.http://www.cisco.com/web/about/security/intelligence/unicast-rpf.html QUESTION 10What does the following access list, which is applied on the external interface FastEthernet 1/0 of the perimeter router, accomplish? router(config)#access-list 101 deny ip 10.0.0.0 0.255.255.255 any logrouter (config)#access-list 101 deny ip 192.168.0.0 0.0.255.255 any logrouter (config)#access-list 101 deny ip 172.16.0.0 0.15.255.255 any logrouter (config)#access-list 101 permit ip any anyrouter (config)#interface fastEthernet 1/0router (config-if)#ip access-group 101 in A. It prevents incoming traffic from IP address ranges 10.0.0.0-10.0.0.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255 and logs any intrusion attempts.B. It prevents the internal network from being used in spoofed denial of service attacks and logs any exit to the Internet.C. It filters incoming traffic from private addresses in order to prevent spoofing and logs any intrusion attempts.D. It prevents private internal addresses to be accessed directly from outside. Answer: CExplanation:The private IP address ranges defined in RFC 1918 are as follows:10.0.0.0 -- 10.255.255.255172.16.0.0 -- 172.31.255.255192.168.0.0 -- 192.168.255.255These IP addresses should never be allowed from external networks into a corporate network as they would only be able to reach the network from the outside via routing problems or if the IP addresses were spoofed. This ACL is used to prevent all packets with a spoofed reserved private source IP address to enter the network. The log keyword also enables logging of this intrusion attempt. **300-101 dumps full version (PDF&VCE):** https://www.lead2pass.com/300-101.html **Large amount of free 300-101 exam questions on Google Drive:** https://drive.google.com/open?id=0B3Syig5i8gpDbHBiVVk1ZVhpOGc You may also need: 300-115 exam dumps: https://drive.google.com/open?id=0B3Syig5i8gpDM0pqaFJWUXVuM2M 300-135 exam dumps: https://drive.google.com/open?id=0B3Syig5i8gpDZmFQVlZDZnpLejA