

[Lead2pass Official Official 210-260 Exam Preparation Download From Lead2pass (281-300)]

2017 September Cisco Official New Released 210-260 Dumps in Lead2pass.com! 100% Free Download! 100% Pass Guaranteed! I was very confused about selecting the best practice test website when preparing for my 210-260 certification exam. Luckily, a friend told me about Lead2pass.com. I passed the 210-260 exam from the first try. Excellent website for free exam dumps! Following questions and answers are all new published by Cisco Official Exam Center: <https://www.lead2pass.com/210-260.html>

QUESTION 281 Which statement about zone-based firewall configuration is true? A. Traffic is implicitly denied by default between interfaces the same zone. B. Traffic that is desired to or sourced from the self-zone is denied by default. C. The zone must be configured before a can be assigned. D. You can assign an interface to more than one interface. Answer: C

QUESTION 282 Refer to the above. Which translation technique does this configuration result in? # nat (inside,outside) dynamic interface A. Static NAT. B. Dynamic NAT. C. Dynamic PAT. D. Twice NAT. Answer: C

QUESTION 283 Which term best describes the concept of preventing the modification of data in transit and in storage? A. Confidentiality. B. Integrity. C. Availability. D. fidelity. Answer: B

Explanation: Integrity for data means that changes made to data are done only by authorized individuals/systems. Corruption of data is a failure to maintain data integrity. Source: Cisco Official Certification Guide, Confidentiality, Integrity, and Availability, p.6

QUESTION 284 Which option is a characteristic of the RADIUS protocol? A. uses TCP. B. offers multiprotocol support. C. combines authentication and authorization in one process. D. supports bi-directional challenge. Answer: C

Explanation: http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml Authentication and Authorization RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization. TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information. During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

QUESTION 285 What do you use when you have a network object or group and want to use an IP address? A. Static NAT. B. Dynamic NAT. C. identity NAT. D. Static PAT. Answer: B

QUESTION 286 What are two challenges faced when deploying host-level IPS? (Choose Two) A. The deployment must support multiple operating systems. B. It does not provide protection for offsite computers. C. It is unable to provide a complete network picture of an attack. D. It is unable to determine the outcome of every attack that it detects. E. It is unable to detect fragmentation attacks. Answer: A, B

Explanation: Advantages of HIPS: The success or failure of an attack can be readily determined. A network IPS sends an alarm upon the presence of intrusive activity but cannot always ascertain the success or failure of such an attack. HIPS does not have to worry about fragmentation attacks or variable Time to Live (TTL) attacks because the host stack takes care of these issues. If the network traffic stream is encrypted, HIPS has access to the traffic in unencrypted form. Limitations of HIPS: There are two major drawbacks to HIPS: + HIPS does not provide a complete network picture: Because HIPS examines information only at the local host level, HIPS has difficulty constructing an accurate network picture or coordinating the events happening across the entire network. + HIPS has a requirement to support multiple operating systems: HIPS needs to run on every system in the network. This requires verifying support for all the different operating systems used in your network. Source: <http://www.ciscopress.com/articles/article.asp?p=1336425&seqNum=3>

QUESTION 287 When AAA login authentication is configured on Cisco routers, which two authentication methods should be used as the final method to ensure that the administrator can still log in to the router in case the external AAA server fails? (Choose two.) A. group RADIUS. B. group TACACS+. C. local. D. krb5. E. enable. F. if-authenticated. Answer: C, E

Explanation: http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/scftplus.html

QUESTION 288 With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.) A. traffic flowing between a zone member interface and any interface that is not a zone member. B. traffic flowing to and from the router interfaces (the self zone). C. traffic flowing among the interfaces that are members of the same zone. D. traffic flowing among the interfaces that are not assigned to any zone. E. traffic flowing between a zone member interface and another interface that belongs in a different zone. F. traffic flowing to the zone member interface that is returned traffic. Answer: B, C, D

Explanation: http://www.cisco.com/en/US/products/sw/secursw/ps1018/products_tech_note09186a00808bc994.shtml Rules For

Applying Zone-Based Policy Firewall Router network interfaces' membership in zones is subject to several rules that govern interface behavior, as is the traffic moving between zone member interfaces: A zone must be configured before interfaces can be assigned to the zone. An interface can be assigned to only one security zone. All traffic to and from a given interface is implicitly blocked when the interface is assigned to a zone, except traffic to and from other interfaces in the same zone, and traffic to any interface on the router. Traffic is implicitly allowed to flow by default among interfaces that are members of the same zone. In order to permit traffic to and from a zone member interface, a policy allowing or inspecting traffic must be configured between that zone and any other zone. The self zone is the only exception to the default deny all policy. All traffic to any router interface is allowed until traffic is explicitly denied. Traffic cannot flow between a zone member interface and any interface that is not a zone member. Pass, inspect, and drop actions can only be applied between two zones. Interfaces that have not been assigned to a zone function as classical router ports and might still use classical stateful inspection/CBAC configuration. If it is required that an interface on the box not be part of the zoning/firewall policy. It might still be necessary to put that interface in a zone and configure a pass all policy (sort of a dummy policy) between that zone and any other zone to which traffic flow is desired. From the preceding it follows that, if traffic is to flow among all the interfaces in a router, all the interfaces must be part of the zoning model (each interface must be a member of one zone or another). The only exception to the preceding deny by default approach is the traffic to and from the router, which will be permitted by default. An explicit policy can be configured to restrict such traffic.

QUESTION 289 Which statement is a benefit of using Cisco IOS IPS? A. It uses the underlying routing infrastructure to provide an additional layer of security. B. It works in passive mode so as not to impact traffic flow. C. It supports the complete signature database as a Cisco IPS sensor appliance. D. The signature database is tied closely with the Cisco IOS image. Answer: A

QUESTION 290 Which command do you enter to enable authentication for OSPF on an interface? A. `router(config-if)#ip ospf message-digest-key 1 md5 CISCOPASSB`. `router(config-router)#area 0 authentication message-digestC`. `router(config-router)#ip ospf authentication-key CISCOPASSD`. `router(config-if)#ip ospf authentication message-digest` Answer: D

QUESTION 291 Which two options are advantages of an application layer firewall? (Choose two.) A. provides high-performance filtering B. makes DoS attacks difficult C. supports a large number of applications D. authenticates devices E. authenticates individuals Answer: BE

Explanation:

[http://www.cisco.com/en/US/prod/collateral/vpndev/ps6032/ps6094/ps6120/prod_white_p](http://www.cisco.com/en/US/prod/collateral/vpndev/ps6032/ps6094/ps6120/prod_white_p aper0900aecd8058ec85.html) Adding Intrusion Prevention Gartner's definition of a next-generation firewall is one that combines firewall filtering and intrusion prevention systems (IPSs). Like firewalls, IPSs filter packets in real time. But instead of filtering based on user profiles and application policies, they scan for known malicious patterns in incoming code, called signatures. These signatures indicate the presence of malware, such as worms, Trojan horses, and spyware. Malware can overwhelm server and network resources and cause denial of service (DoS) to internal employees, external Web users, or both. By filtering for known malicious signatures, IPSs add an extra layer of security to firewall capabilities; once the malware is detected by the IPS, the system will block it from the network. Firewalls provide the first line of defense in any organization's network security infrastructure. They do so by matching corporate policies about users' network access rights to the connection information surrounding each access attempt. If the variables don't match, the firewall blocks the access connection. If the variables do match, the firewall allows the acceptable traffic to flow through the network. In this way, the firewall forms the basic building block of an organization's network security architecture. It pays to use one with superior performance to maximize network uptime for business-critical operations. The reason is that the rapid addition of voice, video, and collaborative traffic to corporate networks is driving the need for firewall engines that operate at very high speeds and that also support application-level inspection. While standard Layer 2 and Layer 3 firewalls prevent unauthorized access to internal and external networks, firewalls enhanced with application-level inspection examine, identify, and verify application types at Layer 7 to make sure unwanted or misbehaving application traffic doesn't join the network. With these capabilities, the firewall can enforce endpoint user registration and authentication and provide administrative control over the use of multimedia applications.

QUESTION 292 Refer to the exhibit. Using a stateful packet firewall and given an inside ACL entry of `permit ip 192.16.1.0 0.0.0.255 any`, what would be the resulting dynamically configured ACL for the return traffic on the outside ACL? A. `permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300B`. `permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300C`. `permit tcp any eq 80 host 192.168.1.11 eq 2300D`. `permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300` Answer: A

QUESTION 293 Which command is used to verify that a VPN connection is established between two endpoints and that the connection is passing? A. `Firewall#sh crypto ipsec saB`. `Firewall#sh crypto isakmp saC`. `Firewall#debug crypto isakmpD`. `Firewall#sh crypto session` Answer: A

QUESTION 294 Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.) A. EAPB. ASCII C. PAPD. PEAPE. MS-CHAPv1F. MS-CHAPv2 Answer: BCE

QUESTION 295 Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISR router? (Choose two.) A. syslogB. SDEEC. FTPD. TFTPE. SSHF. HTTPS Answer: BF

Explanation:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_pa](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html) per0900aecd805c4ea8.html

QUESTION 296 Refer to the below. Which statement about this debug output is true? A. The requesting authentication request came from username GETUSER.B. The TACACS+ authentication request came from a valid user.C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.D. The initiating connection request was being spoofed by a different source address. Answer: B QUESTION 297 Which IOS command is used to define the authentication key for NTP? A. Switch(config)#ntp authentication-key 1 md5 C1sc0B. Switch(config)#ntp trusted-key 1C. Switch(config)#ntp source 192.168.0.1D. Switch(config)#ntp authenticate Answer: A QUESTION 298 Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router? A. aaa accounting network start-stop tacacs+B. aaa accounting system start-stop tacacs+C. aaa accounting exec start-stop tacacs+D. aaa accounting connection start-stop tacacs+E. aaa accounting commands 15 start-stop tacacs+ Answer: C Explanation:

http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html aaa accounting To enable authentication, authorization, and accounting (AAA) accounting of requested services for billing or security purposes when you use RADIUS or TACACS+, use the aaa accounting command in global configuration mode or template configuration mode. To disable AAA accounting, use the no form of this command. aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | list-name | guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} no aaa accounting {auth-proxy | system | network | exec | connection | commands level | dot1x} {default | listname | guarantee-first} [vrf vrf-name] {start-stop | stop-only | none} [broadcast] {radius | group group-name} execRuns accounting for the EXEC shell session.start-stopSends a "start" accounting notice at the beginning of a process and a "stop" accounting notice at the end of a process. The "start" accounting record is sent in the background. The requested user process begins regardless of whether the "start" accounting notice was received by the accounting server. QUESTION 299 What can cause the the state table of a stateful firewall to update? (choose two) A. when a connection is createdB. When a connection's timer has expired within state tableC. when packet is evaluated against the outbound access list and is deniedD. when outbound packets forwarded to outbound interfaceE. when rate-limiting is applied Answer: AB QUESTION 300 On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used? A. used for SSH server/client authentication and encryptionB. used to verify the digital signature of the IPS signature fileC. used to generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISR when accessing it using Cisco Configuration ProfessionalD. used to enable asymmetric encryption on IPsec and SSL VPNsE. used during the DH exchanges on IPsec VPNs Answer: B Explanation:

[http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_pa](http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html) per0900aecd805c4ea8.html Thanks for the high quality 210-260 study guide. Will be back soon for more dumps. 210-260 new questions on Google Drive:

<https://drive.google.com/open?id=0B3Syig5i8gpDYUk3WWFWOEhsSU0> 2017 Cisco 210-260 exam dumps (All 362 Q&As) from Lead2pass: <https://www.lead2pass.com/210-260.html> [100% Exam Pass Guaranteed]