Vendor: Cisco

Exam Code: 210-260

Exam Name: Implementing Cisco Network Security (IINS)

Version: Demo

QUESTION 1
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

Correct Answer: BCD
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 2
Which option is the default value for the Diffie璈ellman group when configuring a site-to-site VPN on an ASA device?

A. Group 1
B. Group 2
C. Group 5
D. Group 7

Correct Answer: B

QUESTION 3
Which two characteristics of an application layer firewall are true? (Choose two)

A. provides protection for multiple applications
B. is immune to URL manipulation
C. provides reverse proxy services
D. provides stateful firewall functionality
E. has low processor usage

Correct Answer: AC

QUESTION 4
Refer to the exhibit. Which statement about this output is true?

```
Oct 13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): port='tty515' list=''
action=LOGIN service=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): console enable - default to
enable password (if any)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): Method=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): continue_login
(user='(undef)')
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): Method=ENABLE
Oct 13 19:46:07.266: AAA/AUTHEN(2600878790): password incorrect
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct 13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
```

A. The user logged into the router with the incorrect username and password.
B. The login failed because there was no default enable password.
C. The login failed because the password entered was incorrect.
D. The user logged in and was given privilege level 15.

Correct Answer: C
Explanation:
http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfaaa.html

debug aaa authentication
To display information on AAA/Terminal Access Controller Access Control System Plus (TACACS+) authentication, use the debug aaa authentication privileged EXEC command. To disable debugging command, use the no form of the command.
debug aaa authentication

no debug aaa authentication
The following is sample output from the debug aaa authentication command. A single EXEC login that uses the "default" method list and the first method, TACACS+, is displayed. The TACACS+ server sends a GETUSER request to prompt for the username and then a GETPASS request to prompt for the password, and finally a PASS response to indicate a successful login. The number 50996740 is the session ID, which is unique for each authentication. Use this ID number to distinguish between different authentications if several are occurring concurrently.

Router# debug aaa authentication
6:50:12: AAA/AUTHEN: create_user user='' ruser='' port='tty19' rem_addr='172.31.60.15' authen_type=1 service=1 priv=1

6:50:12: AAA/AUTHEN/START (0): port='tty19' list='' action=LOGIN service=LOGIN
6:50:12: AAA/AUTHEN/START (0): using "default" list
6:50:12: AAA/AUTHEN/START (50996740): Method=TACACS+
6:50:12: TAC+ (50996740): received authen response status = GETUSER
6:50:12: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN/CONT (50996740): continue_login
6:50:15: AAA/AUTHEN (50996740): status = GETUSER
6:50:15: AAA/AUTHEN (50996740): Method=TACACS+
6:50:15: TAC+: send AUTHEN/CONT packet
6:50:15: TAC+ (50996740): received authen response status = GETPASS
6:50:15: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN/CONT (50996740): continue_login
6:50:20: AAA/AUTHEN (50996740): status = GETPASS
6:50:20: AAA/AUTHEN (50996740): Method=TACACS+
6:50:20: TAC+: send AUTHEN/CONT packet
6:50:20: TAC+ (50996740): received authen response status = PASS
6:50:20: AAA/AUTHEN (50996740): status = PASS

QUESTION 5
What is true about the Cisco IOS Resilient Configuration feature?

A. The feature can be disabled through a remote session
B. There is additional space required to secure the primary Cisco IOS Image file
C. The feature automatically detects image and configuration version mismatch
D. Remote storage is used for securing files

Correct Answer: C

QUESTION 6
A Cisco ASA appliance has three interfaces configured. The first interface is the inside interface with a security level of 100. The second interface is the DMZ interface with a security level of 50. The third interface is the outside interface with a security level of 0. By default, without any access list configured, which five types of traffic are permitted? (Choose five.)

A. outbound traffic initiated from the inside to the DMZ
B. outbound traffic initiated from the DMZ to the outside
C. outbound traffic initiated from the inside to the outside
D. inbound traffic initiated from the outside to the DMZ
E. inbound traffic initiated from the outside to the inside
F. inbound traffic initiated from the DMZ to the inside

G. HTTP return traffic originating from the inside network and returning via the outside interface
H. HTTP return traffic originating from the inside network and returning via the DMZ interface
I. HTTP return traffic originating from the DMZ network and returning via the inside interface
J. HTTP return traffic originating from the outside network and returning via the inside interface

Correct Answer: ABCGH
Explanation:
http://www.cisco.com/en/US/docs/security/asa/asa70/configuration/guide/intparam.html

Security Level Overview
Each interface must have a security level from 0 (lowest) to 100 (highest). For example, you should assign your most secure network, such as the inside host network, to level 100. While the outside network connected to the Internet can be level 0. Other networks, such as DMZs can be in between. You can assign interfaces to the same security level. See the "Allowing Communication Between Interfaces on the Same Security Level" section for more information.
The level controls the following behavior:

Network access -- By default, there is an implicit permit from a higher security interface to a lower security interface (outbound). Hosts on the higher security interface can access any host on a lower security interface. You can limit access by applying an access list to the interface. If you enable communication for same security interfaces (see the "Allowing Communication Between Interfaces on the Same Security Level" section), there is an implicit permit for interfaces to access other interfaces on the same security level or lower.

Inspection engines -- Some inspection engines are dependent on the security level. For same security interfaces, inspection engines apply to traffic in either direction. 琀etBIOS inspection engine--Applied only for outbound connections. 瑩raServ inspection engine -- If a control connection for the OraServ port exists between a pair of hosts, then only an inbound data connection is permitted through the security appliance.
Filtering--HTTP(S) and FTP filtering applies only for outbound connections (from a higher level to a lower level).
For same security interfaces, you can filter traffic in either direction. 種AT control -- When you enable NAT control, you must configure NAT for hosts on a higher security interface (inside) when they access hosts on a lower security interface (outside).
Without NAT control, or for same security interfaces, you can choose to use NAT between any interface, or you can choose not to use NAT. Keep in mind that configuring NAT for an outside interface might require a special keyword. 積stablished command -- This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.
For same security interfaces, you can configure established commands for both directions.

QUESTION 7
Which three options are common examples of AAA implementation on Cisco routers? (Choose three.)

A. authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
B. authenticating administrator access to the router console port, auxiliary port, and vty ports
C. implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
D. tracking Cisco NetFlow accounting statistics
E. securing the router by locking down all unused services
F. performing router commands authorization using TACACS+

Correct Answer: ABF
Explanation:
http://www.cisco.com/en/US/products/ps6638/products_data_sheet09186a00804fe332.htm l

Need for AAA Services
Security for user access to the network and the ability to dynamically define a user's profile to gain access to network resources has a legacy dating back to asynchronous dial access. AAA network security services provide the primary framework through which a network administrator can set up access control on network points of entry or network access servers, which is usually the function of a router or access server.

Authentication identifies a user; authorization determines what that user can do; and accounting monitors the network usage time for billing purposes. AAA information is typically stored in an external database or remote server such as RADIUS or TACACS+.
The information can also be stored locally on the access server or router. Remote security servers, such as RADIUS and TACACS+, assign users specific privileges by associating attribute-value (AV) pairs, which define the access rights with the appropriate user. All authorization methods must be defined through AAA.

QUESTION 8
Which two devices are components of the BYOD architectural framework?

A. Prime Infrastructure
B. Nexus 7010 Switch
C. Cisco 3945 Router
D. Wireless Access Points
E. Identity Services Engine

Correct Answer: AE

QUESTION 9
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

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

TACACS+ Authentication Examples
The following example shows how to configure TACACS+ as the security protocol for PPP authentication:
aaa new-model
aaa authentication ppp test group tacacs+ local
tacacs-server host 10.1.2.3

tacacs-server key goaway
interface serial 0
ppp authentication chap pap test
The lines in the preceding sample configuration are defined as follows:
The aaa new-model command enables the AAA security services. 秘he aaa authentication command defines a method list, "test," to be used on serial interfaces running PPP.
The keyword group tacacs+ means that authentication will be done through TACACS+. If TACACS+ returns an ERROR of some sort during authentication, the keyword local indicates that authentication will be attempted using the local database on the network access server.
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800946a3.shtml
Authentication Start to configure TAC+ on the router. Enter enable mode and type configure terminal before the command set. This command syntax ensures that you are not locked out of the router initially, providing the tac_plus_executable is not running:
!--- Turn on TAC+.
aaa new-model
enable password whatever
!--- These are lists of authentication methods.
!--- "linmethod", "vtymethod", "conmethod", and
!--- so on are names of lists, and the methods
!--- listed on the same lines are the methods
!--- in the order to be tried. As used here, if
!--- authentication fails due to the
!--- tac_plus_executable not being started, the
!--- enable password is accepted because
!--- it is in each list.
!
aaa authentication login linmethod tacacs+ enable
aaa authentication login vtymethod tacacs+ enable
aaa authentication login conmethod tacacs+ enable

QUESTION 10
Which product can be used to provide application layer protection for TCP port 25 traffic?

A. ESA
B. CWS
C. WSA
D. ASA

Correct Answer: A

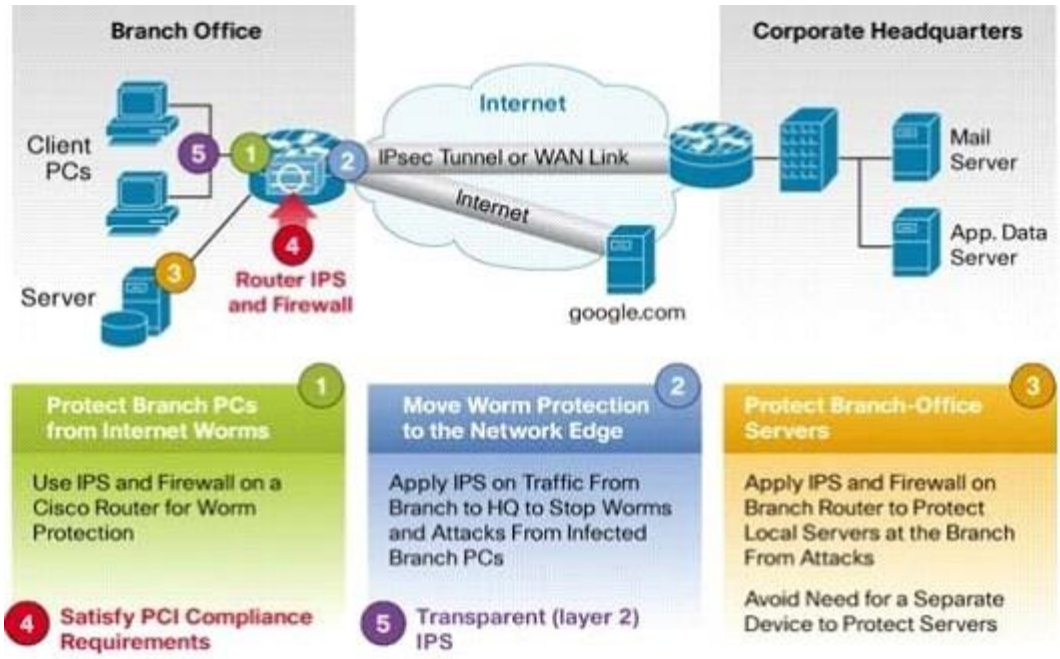
QUESTION 11
Which statement is a benefit of using Cisco IOS IPS?

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.

Correct Answer: A
Explanation:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/product_data_sheet0900aecd803137cf.html

Product Overview
In today's business environment, network intruders and attackers can come from outside or inside the network.
They can launch distributed denial-of-service attacks, they can attack Internet connections, and they can exploit network and host vulnerabilities. At the same time, Internet worms and viruses can spread across the world in a matter of minutes. There is often no time to wait for human intervention-the network itself must possess the intelligence to recognize and mitigate these attacks, threats, exploits, worms and viruses. Cisco IOS Intrusion Prevention System (IPS) is an inline, deep-packet inspection-based solution that enables Cisco IOS Software to effectively mitigate a wide range of network attacks. While it is common practice to defend against attacks by inspecting traffic at data centers and corporate headquarters, distributing the network level defense to stop malicious traffic close to its entry point at branch or telecommuter offices is also critical.

Cisco IOS IPS: Major Use Cases and Key Benefits
IOS IPS helps to protect your network in 5 ways:



Key Benefits:
Provides network-wide, distributed protection from many attacks, exploits, worms and viruses exploiting vulnerabilities in operating systems and applications. ?Eliminates the need for a standalone IPS device at branch and telecommuter offices as well as small and medium-sized business networks.
Unique, risk rating based signature event action processor dramatically improves the ease of management of IPS policies.
Offers field-customizable worm and attack signature set and event actions. ?Offers inline inspection of traffic passing through any combination of router LAN and WAN interfaces in both directions.
Works with Cisco IOS?Firewall, control-plane policing, and other Cisco IOS Software security features to protect the router and networks behind the router. ?Supports more than 3700 signatures from the same signature database available for Cisco Intrusion Prevention System (IPS) appliances.

QUESTION 12
What configure mode you used for the command ip ospf authentication-key c1$c0?

A. global
B. privileged
C. in-line
D. Interface

Correct Answer: D
Explanation:
ip ospf authentication-key is used under interface configuration mode, so it's in interface level, under global configuration mode. If it asks about interface level then choose that.
interface Serial0
ip address 192.16.64.1 255.255.25

QUESTION 13
Which option is the cloud based security service from Cisco that provides URL filtering web browsing content security, and roaming user protection?

A. Cloud web security
B. Cloud web Protection
C. Cloud web Service
D. Cloud advanced malware protection

Correct Answer: A

QUESTION 14
When is the default deny all policy an exception in zone-based firewalls?

A. When traffic traverses two interfaces in the same zone
B. When traffic terminates on the router via the self zone
C. When traffic sources from the router via the self zone
D. When traffic traverses two interfaces in different zones

Correct Answer: A

QUESTION 15
Which two characteristics of the TACACS+ protocol are true? (Choose two.)

A. uses UDP ports 1645 or 1812
B. separates AAA functions
C. encrypts the body of every packet
D. offers extensive accounting capabilities
E. is an open RFC standard protocol

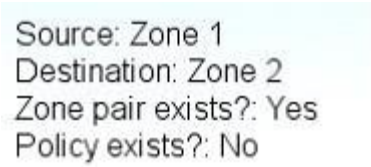
Correct Answer: BC
Explanation:
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml

Packet Encryption
RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party. TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.
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 16
Which option is the resulting action in a zone-based policy firewall configuration with these conditions?



A. no impact to zoning or policy
B. no policy lookup (pass)
C. drop
D. apply default policy

Correct Answer: C
Explanation:
http://www.cisco.com/en/US/docs/ios-xml/ios/sec_data_zbf/configuration/xe-3s/sec-zone- pol-fw.html

Zone Pairs
A zone pair allows you to specify a unidirectional firewall policy between two security zones. To define a zone pair, use the zone-pair security command. The direction of the traffic is specified by source and destination zones. The source and destination zones of a zone pair must be security zones.

You can select the default or self zone as either the source or the destination zone. The self zone is a systemdefined zone which does not have any interfaces as members. A zone pair that

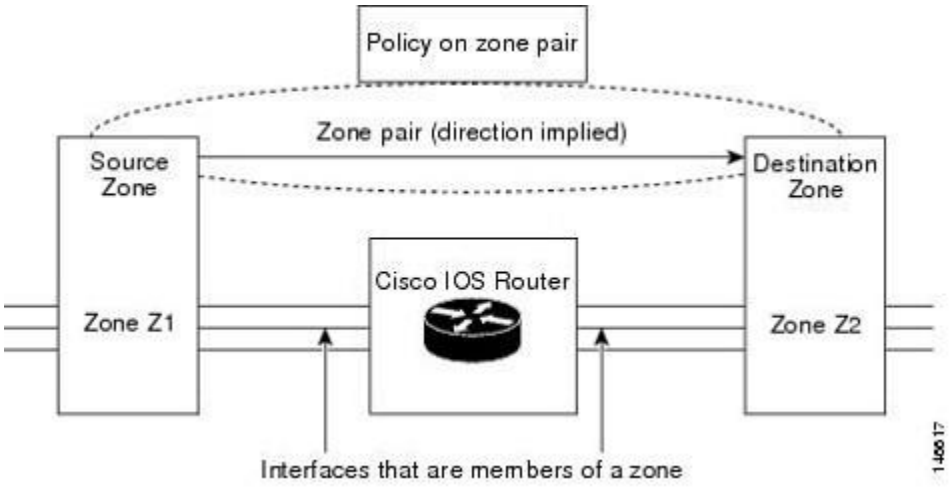
includes the self zone, along with the associated policy, applies to traffic directed to the device or traffic generated by the device. It does not apply to traffic through the device.

The most common usage of firewall is to apply them to traffic through a device, so you need at least two zones (that is, you cannot use the self zone).

To permit traffic between zone member interfaces, you must configure a policy permitting (or inspecting) traffic between that zone and another zone. To attach a firewall policy map to the target zone pair, use the servicepolicy type inspect command.

The figure below shows the application of a firewall policy to traffic flowing from zone Z1 to zone Z2, which means that the ingress interface for the traffic is a member of zone Z1 and the egress interface is a member of zone Z2.

Figure 2. Zone Pairs



If there are two zones and you require policies for traffic going in both directions (from Z1 to Z2 and Z2 to Z1), you must configure two zone pairs (one for each direction).

If a policy is not configured between zone pairs, traffic is dropped. However, it is not necessary to configure a zone pair and a service policy solely for the return traffic. By default, return traffic is not allowed. If a service policy inspects the traffic in the forward direction and there is no zone pair and service policy for the return traffic, the return traffic is inspected. If a service policy passes the traffic in the forward direction and there is no zone pair and service policy for the return traffic, the return traffic is dropped. In both these cases, you need to configure a zone pair and a service policy to allow the return traffic. In the above figure, it is not mandatory that you configure a zone pair source and destination for allowing return traffic from Z2 to Z1. The service policy on Z1 to Z2 zone pair takes care of it.

QUESTION 17
On Cisco ISR routers, for what purpose is the realm-cisco.pub public encryption key used?

A. used for SSH server/client authentication and encryption
B. used to verify the digital signature of the IPS signature file
C. used to generate a persistent self-signed identity certificate for the ISR so administrators can authenticate the ISR when accessing it using Cisco Configuration Professional
D. used to enable asymmetric encryption on IPsec and SSL VPNs

E. used during the DH exchanges on IPsec VPNs

Correct Answer: B
Explanation:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6634/prod_white_paper0900aecd805c4ea8.html

Step 1: Downloading IOS IPS files
The first step is to download IOS IPS signature package files and public crypto key from Cisco.com.

Step 1.1: Download the required signature files from Cisco.com to your PC ?Location:
http://tools.cisco.com/support/downloads/go/Model.x?mdfid=281442967&mdfLevel=Software%20Family&treeName=Security&modelName=Cisco%20IOS%20Intrusion%20Prevention%20System%20Feature%20Software&treeMdfId=268438162

Files to download:
IOS-Sxxx-CLI.pkg: Signature package - download the latest signature package. realm-cisco.pub.key.txt: Public Crypto key - this is the crypto key used by IOS IPS

QUESTION 18
Refer to the below. Which statement about this debug output is true?

```
Router# debug tacacs

14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

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.

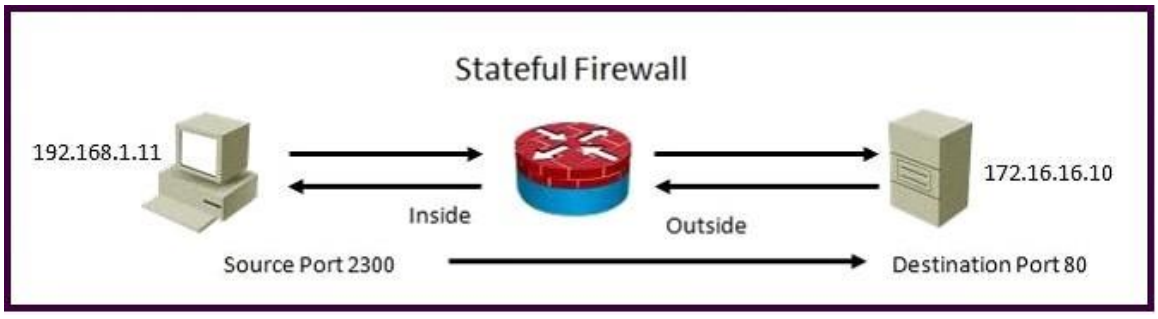
D. The initiating connection request was being spoofed by a different source address.

Correct Answer: B
Explanation:
http://www.cisco.com/en/US/docs/ios/12_2/debug/command/reference/dbfser.html

debug tacacs
To display information associated with the TACACS, use the debug tacacs privileged EXEC command. The no form of this command disables debugging output.
debug tacacs
no debug tacacs
The following is sample output from the debug tacacs command for a TACACS login attempt that was successful, as indicated by the status PASS:

Router# debug tacacs
14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source 10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15 (AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15 (AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15 (AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15

QUESTION 19
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 2300
B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300
C. permit tcp any eq 80 host 192.168.1.11 eq 2300
D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

Correct Answer: A

Explanation:
http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.1/user/guide/fwinsp.html

Understanding Inspection Rules
Inspection rules configure Context-Based Access Control (CBAC) inspection commands. CBAC inspects traffic that travels through the device to discover and manage state information for TCP and UDP sessions. The device uses this state information to create temporary openings to allow return traffic and additional data connections for permissible sessions.
CBAC creates temporary openings in access lists at firewall interfaces. These openings are created when inspected traffic exits your internal network through the firewall. The openings allow returning traffic (that would normally be blocked) and additional data channels to enter your internal network back through the firewall. The traffic is allowed back through the firewall only if it is part of the same session as the original traffic that triggered inspection when exiting through the firewall.

Inspection rules are applied after your access rules, so any traffic that you deny in the access rule is not inspected. The traffic must be allowed by the access rules at both the input and output interfaces to be inspected. Whereas access rules allow you to control connections at layer 3 (network, IP) or 4 (transport, TCP or UDP protocol), you can use inspection rules to control traffic using application-layer protocol session information.

For all protocols, when you inspect the protocol, the device provides the following functions:
Automatically opens a return path for the traffic (reversing the source and destination addresses), so that you do not need to create an access rule to allow the return traffic. Each connection is considered a session, and the device maintains session state information and allows return traffic only for valid sessions. Protocols that use TCP contain explicit session information, whereas for UDP applications, the device models the equivalent of a session based on the source and destination addresses and the closeness in time of a sequence of UDP packets.

These temporary access lists are created dynamically and are removed at the end of a session.
Tracks sequence numbers in all TCP packets and drops those packets with sequence numbers that are not within expected ranges.

Uses timeout and threshold values to manage session state information, helping to determine when to drop sessions that do not become fully established. When a session is dropped, or reset, the device informs both the source and destination of the session to reset the connection, freeing up resources and helping to mitigate potential Denial of Service (DoS) attacks.

QUESTION 20
Which option is a weakness in an information system that an attacker might leverage to gain unauthorized access to the system or its data?

A. hack
B. mitigation
C. risk
D. vulnerability
E. exploit

Correct Answer: D
Explanation:
vulnerability A flaw or weakness in a system's design or implementation that could be exploited.