LEAD2PASS
First Test, First Pass!

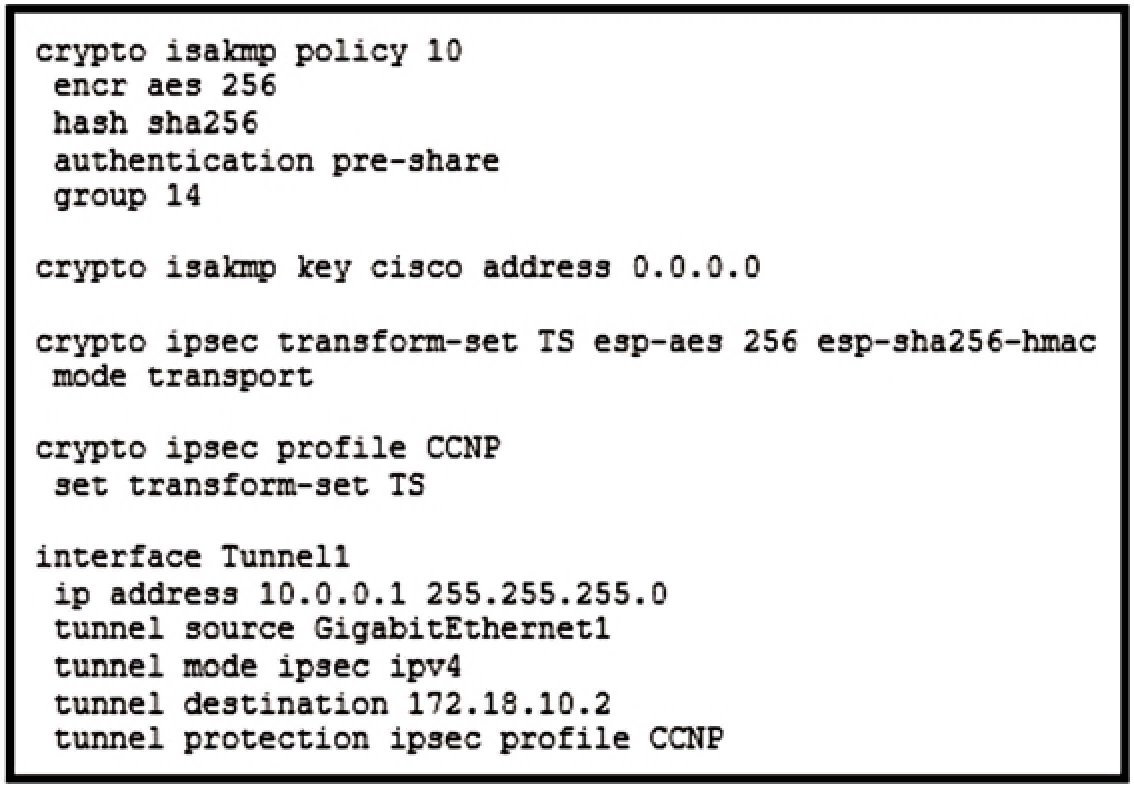
Vendor: Cisco

Exam Code: 300-730

Exam Name: Implementing Secure Solutions with Virtual Private Networks (SVPN)

Version: DEMO

QUESTION 1
Refer to the exhibit. Which VPN technology is used in the exhibit?



```
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14

crypto isakmp key cisco address 0.0.0.0

crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode transport

crypto ipsec profile CCNP
 set transform-set TS

interface Tunnel1
 ip address 10.0.0.1 255.255.255.0
 tunnel source GigabitEthernet1
 tunnel mode ipsec ipv4
 tunnel destination 172.18.10.2
 tunnel protection ipsec profile CCNP
```

A. DVTI
B. VTI
C. DMVPN
D. GRE

Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_vpnips/configuration/zZ-Archive/IPsec_Virtual_Tunnel_Interface.html#GUID-EB8C433B-2394-42B9-997F-B40803E58A91

QUESTION 2
What is a requirement for smart tunnels to function properly?

A. Java or ActiveX must be enabled on the client machine.
B. Applications must be UDP.
C. Stateful failover must not be configured.
D. The user on the client machine must have admin access.

Answer: A
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/111007-smart-tunnel-asa-00.html

QUESTION 3
Where is split tunneling defined for IKEv2 remote access clients on a Cisco router?

A. IKEv2 authorization policy
B. Group Policy
C. virtual template
D. webvpn context

Answer: A
Explanation:
IKEv2 Authorization Policy
Source (Step 13):
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html
Webvpn is for SSL remote access VPN's and the question asks about an IKEv2 remote access

QUESTION 4
Which technology is used to send multicast traffic over a site-to-site VPN?

A. GRE over IPsec on IOS router
B. GRE over IPsec on FTD
C. IPsec tunnel on FTD
D. GRE tunnel on ASA

Answer: A
Explanation:
The GRE over IPsec implementations on Cisco documents refers to Routers.

QUESTION 5
On a FlexVPN hub-and-spoke topology where spoke-to-spoke tunnels are not allowed, which command is needed for the hub to be able to terminate FlexVPN tunnels?

A. interface virtual-access
B. ip nhrp redirect
C. interface tunnel
D. interface virtual-template

Answer: D
Explanation:
Spoke-to-Spoke traffic is not allowed and wanted, therefore redirect is not needed. But FlexVPN uses Virtual Templates to create Virtual Access interfaces for each connected Spoke.

QUESTION 6
Which two changes must be made in order to migrate from DMVPN Phase 2 to Phase 3 when EIGRP is configured? (Choose two.)

A. Add NHRP shortcuts on the hub.
B. Add NHRP redirects on the spoke.
C. Disable EIGRP next-hop-self on the hub.

D. Enable EIGRP next-hop-self on the hub.
E. Add NHRP redirects on the hub.

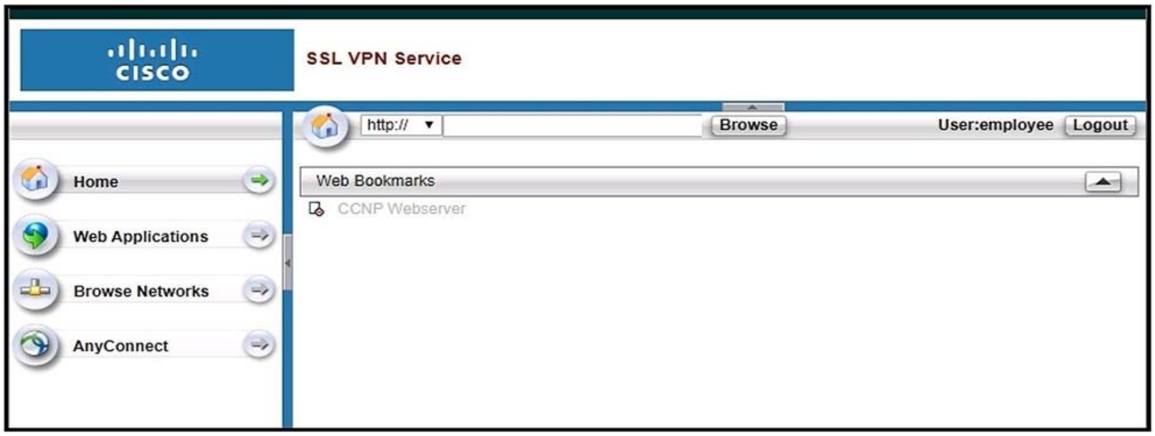
Answer: DE
Explanation:
DMVPN disables the EIRGP next-hop-self with "no ip next-hop-self eigrp xxx" in DMVPN phase 2, and to go from Phase 2 to 3 you need use the NHRP protocol, and again enable EIRGP next-hop-self with "ip next-hop-self eigrp 134" under the tunnel interface.
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_conn_dmvpn/configuration/15-mt/sec-conn-dmvpn-15-mt-book/sec-conn-dmvpn-dmvpn.html#GUID-BF561439-BCC0-4AAF-80D9-1F7876CB7B81

QUESTION 7
Which two types of web resources or protocols are enabled by default on the Cisco ASA Clientless SSL VPN portal? (Choose two.)

A. HTTP
B. ICA (Citrix)
C. VNC
D. RDP
E. CIFS

Answer: AE
Explanation:
You will not see an option of RDP, VNC, SSH, and/or Telnet unless the appropriate client/server plug-in has been installed first.
https://www.cisco.com/c/en/us/td/docs/security/asa/asa94/config-guides/cli/vpn/asa-94-vpn-config/webvpn-configure-gateway.html

QUESTION 8
Refer to the exhibit. Based on the exhibit, why are users unable to access CCNP Webserver bookmark?

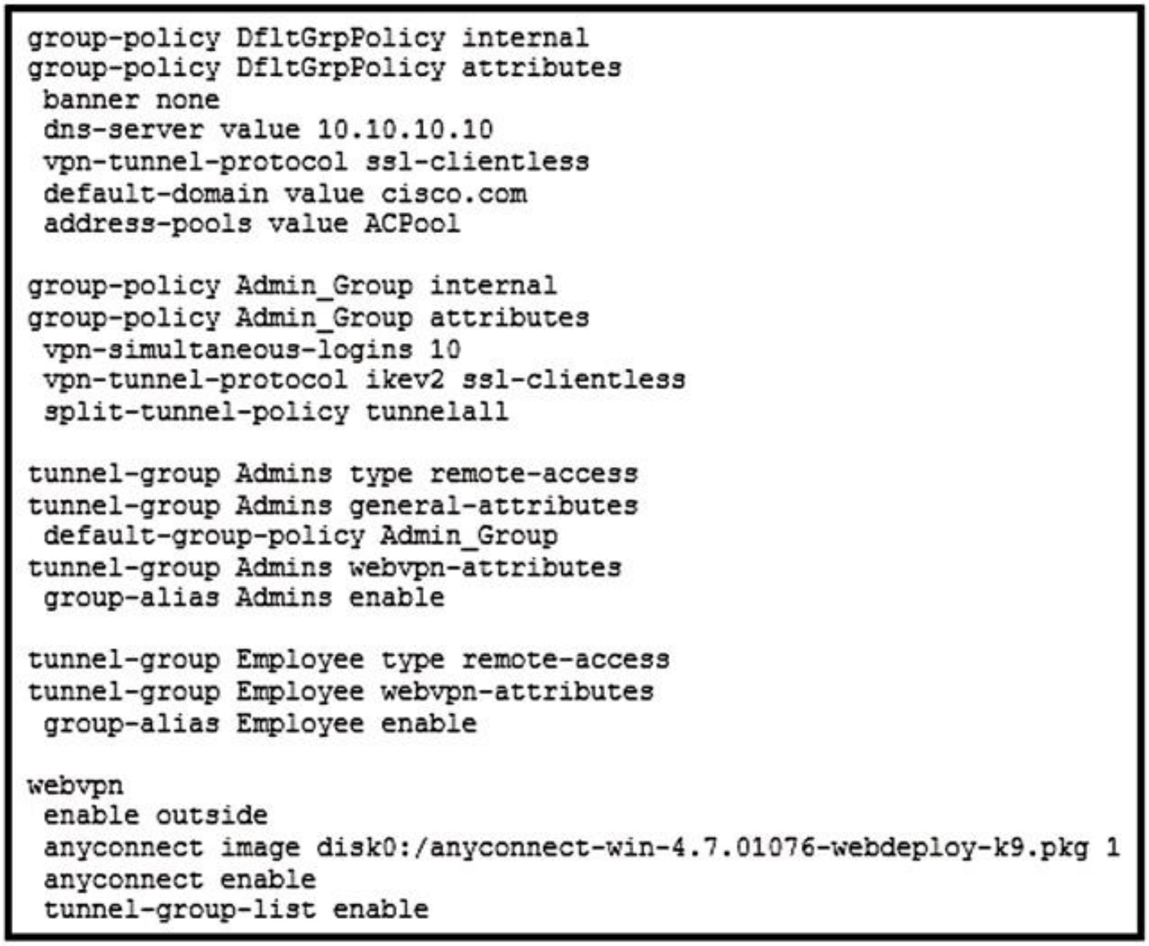


A. The URL is being blocked by a WebACL.
B. The ASA cannot resolve the URL.
C. The bookmark has been disabled.
D. The user cannot access the URL.

Answer: B
Explanation:
WebVPN Clients Cannot Hit Bookmarks and is Grayed Out
Problem
If these bookmarks were configured for users to sign in to the clientless VPN, but on the home screen under "Web Applications" they show up as grayed out, how can I enable these HTTP links so that the users are able to click them and go into the particular URL?

Solution
You should first make sure that the ASA can resolve the websites through DNS. Try to ping the websites by name. If the ASA cannot resolve the name, the link is grayed out. If the DNS servers are internal to your network, configure the DNS domain-lookup private interface.
https://www.cisco.com/c/en/us/support/docs/security-vpn/webvpn-ssl-vpn/119417-config-asa-00.html#anc15

QUESTION 9
Refer to the exhibit. Which VPN technology is allowed for users connecting to the Employee tunnel group?



```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 dns-server value 10.10.10.10
 vpn-tunnel-protocol ssl-clientless
 default-domain value cisco.com
 address-pools value ACPool

group-policy Admin_Group internal
group-policy Admin_Group attributes
 vpn-simultaneous-logins 10
 vpn-tunnel-protocol ikev2 ssl-clientless
 split-tunnel-policy tunnelall

tunnel-group Admins type remote-access
tunnel-group Admins general-attributes
 default-group-policy Admin_Group
tunnel-group Admins webvpn-attributes
 group-alias Admins enable

tunnel-group Employee type remote-access
tunnel-group Employee webvpn-attributes
 group-alias Employee enable

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-4.7.01076-webdeploy-k9.pkg 1
 anyconnect enable
 tunnel-group-list enable
```

A. SSL AnyConnect
B. IKEv2 AnyConnect

C. crypto map
D. clientless

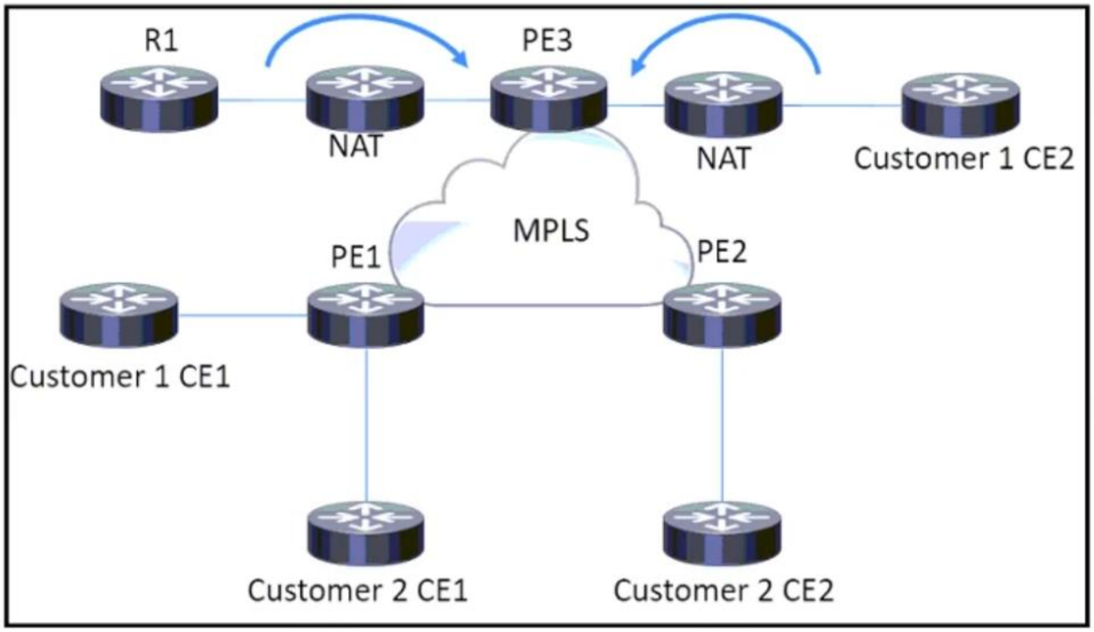
Answer: D
Explanation:
The tunnel-group Employee has no entry for a specific default-group-policy as with the Admin-Group.
The group-policy DfltGrpPolicy is used instead. This permits only ssl-clientless.

QUESTION 10
Which two types of SSO functionality are available on the Cisco ASA without any external SSO servers? (Choose two.)

A. SAML
B. NTLM
C. Kerberos
D. OAuth 2.0
E. HTTP Basic

Answer: BE
Explanation:
The auto-signon command is a single sign-on method for users of clientless SSL VPN sessions. It passes the login credentials (username and password) to internal servers for authentication using NTLM authentication, basic authentication, or both. Multiple auto-signon commands can be entered and are processed according to the input order (early commands take precedence).
https://www.cisco.com/c/en/us/td/docs/security/asa/asa916/configuration/vpn/asa-916-vpn-config/webvpn-configure-policy-groups.html#ID-2439-00001438

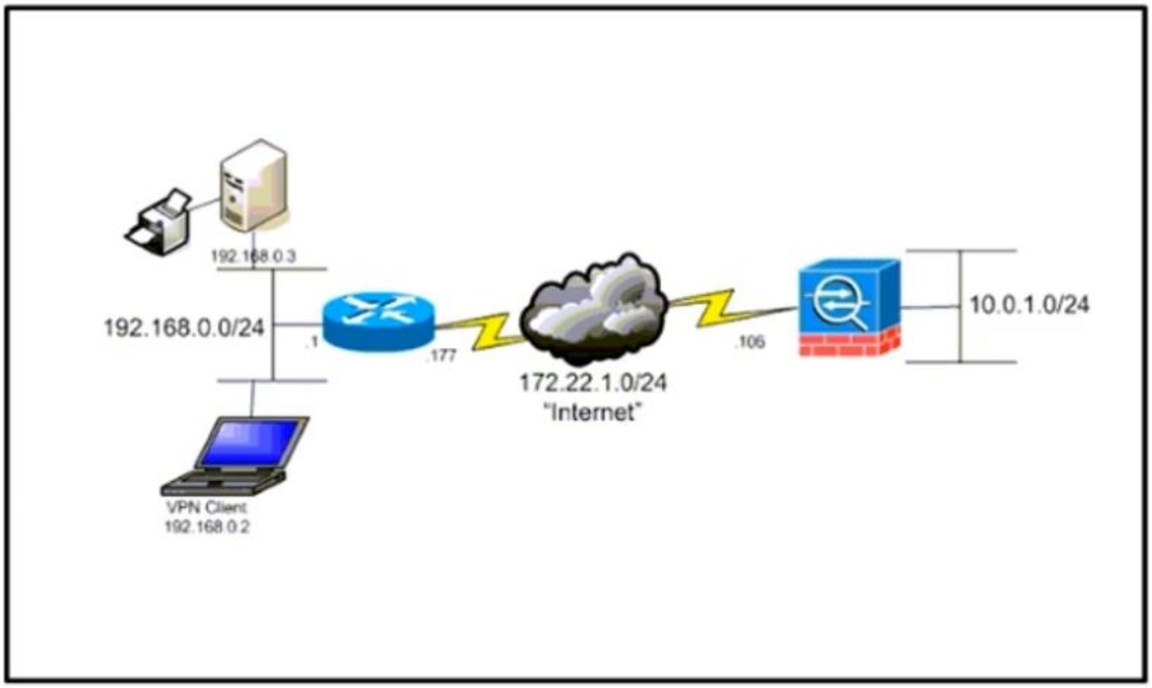
QUESTION 11
Refer to the exhibit. Which component must be configured on routers for a GETVPN deployment work properly?



A. PE3: Key Server - Customer 2 CEs: Group Members
B. Customer 1 CE1: Key Server - R1 and Customer 1 CE2: Group Members
C. R1: Key Server - Customer 1 CEs: Group Members
D. PE3: Key Server - all CEs: Group Members

Answer: A

QUESTION 12
Refer to the exhibit. The network administrator must allow the Cisco AnyConnect Secure Mobility Client to securely access the corporate resources via IKEv2 and print locally. Traffic that is destined for the Internet must still be tunneled to the Cisco ASA. Which configuration does the administrator use to accomplish this goal?



A. Split exclude policy with a deny for 192.168.0.3/32.
B. Split exclude policy with a permit for 0.0.0.0/32.
C. Tunnel all policy.
D. Split include policy with a permit for 192.168.0.0/24.

Answer: B

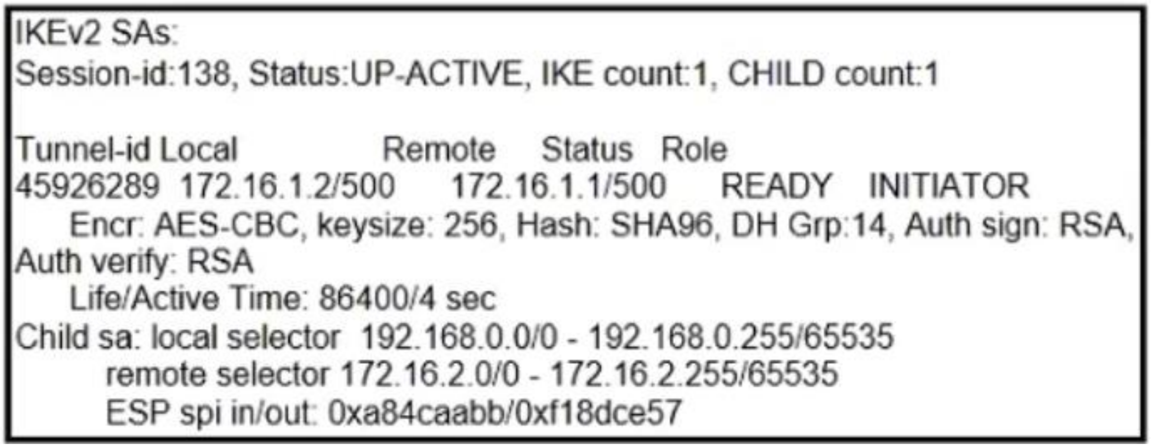
QUESTION 13
Over the weekend, an administrator upgraded the Cisco ASA image on the firewalls and noticed that users cannot connect to the headquarters site using Cisco AnyConnect. What is the solution for this issue?

A. Upgrade the Cisco AnyConnect client version to be compatible with the Cisco ASA software image.
B. Upgrade the Cisco AnyConnect Network Access module to be compatible with the Cisco ASA

software image.
C. Upgrade the Cisco AnyConnect client driver to be compatible with the Cisco ASA software image.
D. Upgrade the Cisco AnyConnect Start Before Logon module to be compatible with the Cisco ASA software image.

Answer: B

QUESTION 14
Refer to the exhibit. A Cisco ASA is configured as a client to a router running as a FlexVPN server. The router is configured with a virtual template to terminate FlexVPN clients. Traffic between networks 192.168.0.0/24 and 172.16.20.0/24 does not work as expected. Based on the show crypto ikev2 sa output collected from the Cisco ASA in the exhibit, what is the solution to this issue?



```
IKEv2 SAs:
Session-id:138, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local              Remote      Status   Role
45926289  172.16.1.2/500     172.16.1.1/500     READY    INITIATOR
     Encr: AES-CBC, keysize: 256, Hash: SHA96, DH Grp:14, Auth sign: RSA,
Auth verify: RSA
     Life/Active Time: 86400/4 sec
Child sa: local selector  192.168.0.0/0 - 192.168.0.255/65535
        remote selector 172.16.2.0/0 - 172.16.2.255/65535
        ESP spi in/out: 0xa84caabb/0xf18dce57
```

A. Modify the crypto ACL on the router to permit network 192.168.0.0/24 to network 172.16.20.0/24.
B. Modify the crypto ACL on the ASA to permit network 192.168.0.0/24 to network 172.16.20.0/24.
C. Modify the crypto ACL on the ASA to permit network 172.16.20.0/24 to network 192.168.0.0/24.
D. Modify the crypto ACL on the router to permit network 172.16.20.0/24 to network 192.168.0.0/24.

Answer: C

QUESTION 15
A network engineer has almost finished setting up a clientless VPN that allows remote users to access internal HTTP servers. Users must enter their username and password twice: once on the clientless VPN web portal and again to log in to internal HTTP servers. The Cisco ASA and the HTTP servers use the same Active Directory server to authenticate users. Which next step must be taken to allow users to enter their password only once?

A. Use LDAPS and add password management to the clientless tunnel group.
B. Configure auto-sign-on using NTLM authentication.
C. Set up the Cisco ASA to authenticate users via a SAML 2.0 IDP.
D. Create smart tunnels for the HTTP servers.

Answer: B

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.lead2pass.com/all-products.html

10% Discount Coupon Code: ASTR14