- **Vendor:** Cisco
- **Exam Code:** 300-730
- **Exam Name:** Implementing Secure Solutions with Virtual Private Networks (SVPN)
- **New Updated Questions from Braindump2go (Updated in May/2020)**

Visit Braindump2go and Download Full Version 300-730 Exam Dumps

QUESTION 45
Which feature allows the ASA to handle nonstandard applications and web resources so that they display correctly over a clientless SSL VPN connection?

A. single sign-on
B. Smart Tunnel
C. WebType ACL
D. plug-ins

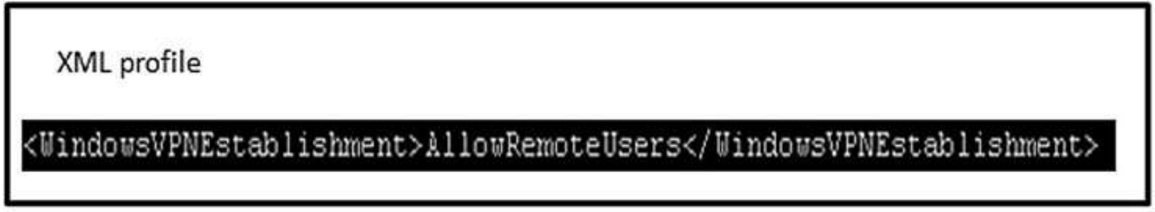
Answer: B
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa90/configuration/guide/asa_90_cli_config/vpn_clientless_ssl.html#29951

QUESTION 46
Which command automatically initiates a smart tunnel when a user logs in to the WebVPN portal page?

A. auto-upgrade
B. auto-connect
C. auto-start
D. auto-run

Answer: C
Explanation:
https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/vpn/asa_91_vpn_config/webvpn-configure-policy-group.html

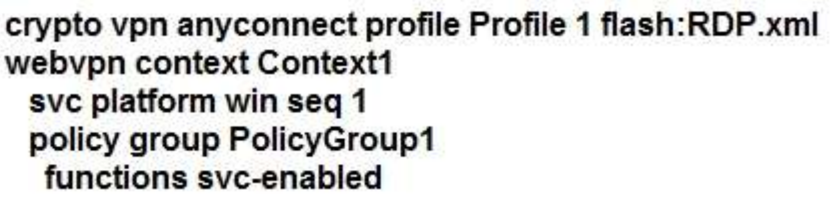
QUESTION 47
Refer to the exhibit. The customer must launch Cisco AnyConnect in the RDP machine. Which IOS configuration accomplishes this task?



XML profile

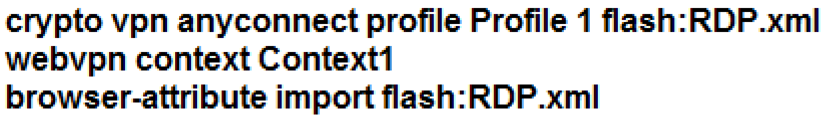
```
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
```

A.



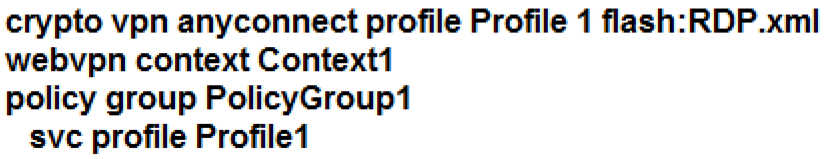
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
  svc platform win seq 1
  policy group PolicyGroup1
    functions svc-enabled
```

B.



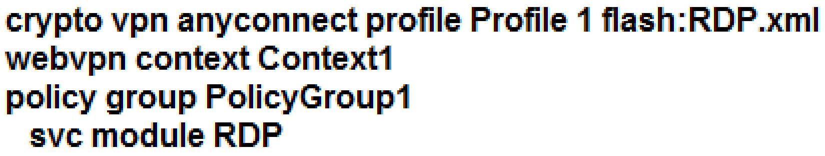
```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
browser-attribute import flash:RDP.xml
```

C.



```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc profile Profile1
```

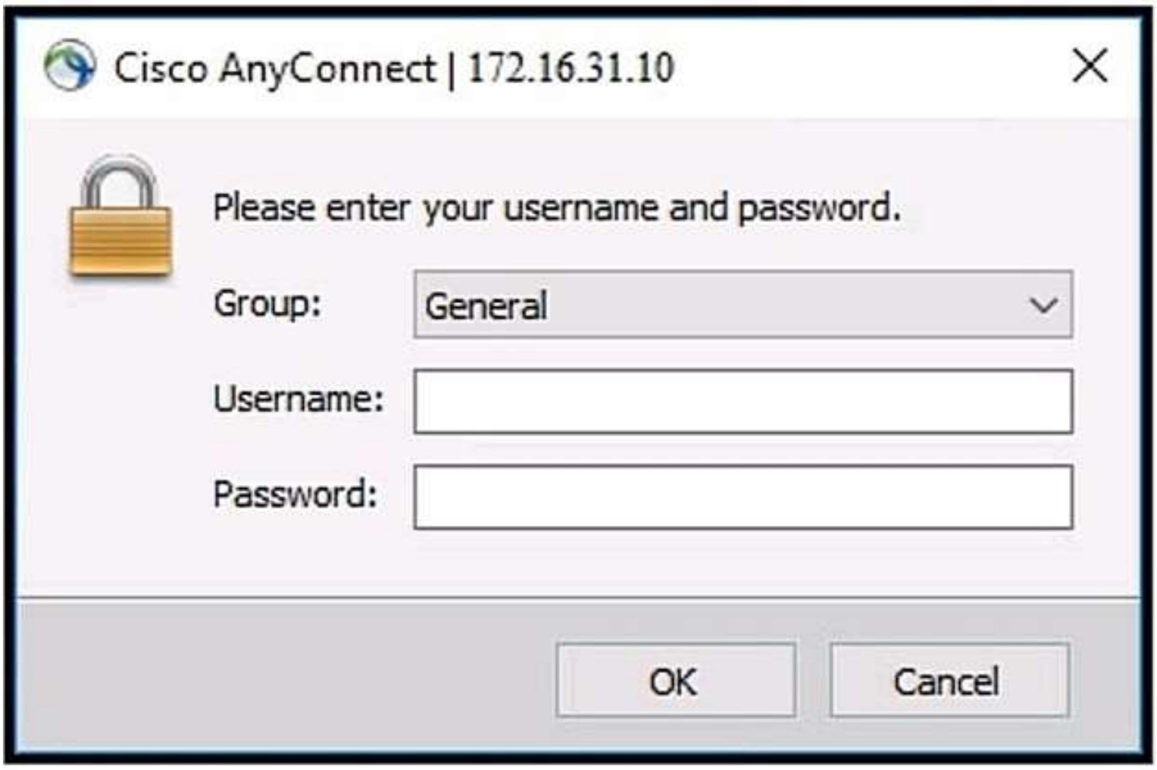
D.



```
crypto vpn anyconnect profile Profile 1 flash:RDP.xml
webvpn context Context1
policy group PolicyGroup1
  svc module RDP
```

Answer: C
Explanation:
https://community.cisco.com/t5/vpn/starting-anyconnect-vpn-through-rdp-session-on-cisco-891/td-p/2128284

QUESTION 48
Refer to the exhibit. Which two commands under the tunnel-group webvpn-attributes result in a Cisco AnyConnect user receiving the AnyConnect prompt in the exhibit? (Choose two.)



Cisco AnyConnect | 172.16.31.10

Please enter your username and password.

Group: General

Username:

Password:

A. group-url https://172.16.31.10/General enable
B. group-policy General internal

C. authentication aaa
D. authentication certificate
E. group-alias General enable

Answer: BE

QUESTION 49
Which two statements are true when designing a SSL VPN solution using Cisco AnyConnect? (Choose two.)

A. The VPN server must have a self-signed certificate.
B. A SSL group pre-shared key must be configured on the server.
C. Server side certificate is optional if using AAA for client authentication.
D. The VPN IP address pool can overlap with the rest of the LAN networks.
E. DTLS can be enabled for better performance.

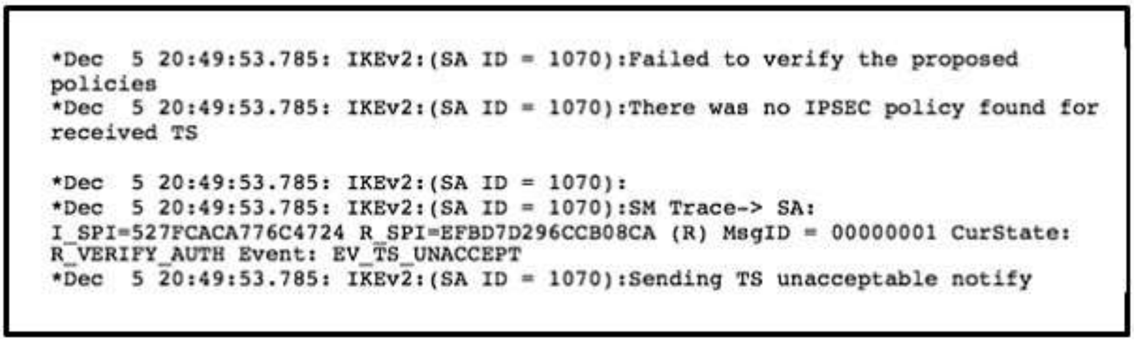
Answer: DE

QUESTION 50
An engineer is configuring IPsec VPN and wants to choose an authentication protocol that is reliable and supports ACK and sequence.
Which protocol accomplishes this goal?

A. IKEv1
B. AES-192
C. ESP
D. AES-256

Answer: C

QUESTION 51
Refer to the exhibit. What is the problem with the IKEv2 site-to-site VPN tunnel?



```
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):Failed to verify the proposed
policies
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):There was no IPSEC policy found for
received TS

*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):SM Trace-> SA:
I_SPI=527FCACA776C4724 R_SPI=EFBD7D296CCB08CA (R) MsgID = 00000001 CurState:
R_VERIFY_AUTH Event: EV_TS_UNACCEPT
*Dec  5 20:49:53.785: IKEv2:(SA ID = 1070):Sending TS unacceptable notify
```

A. incorrect PSK
B. crypto access list mismatch
C. incorrect tunnel group
D. crypto policy mismatch
E. incorrect certificate

Answer: B

QUESTION 52
Which requirement is needed to use local authentication for Cisco AnyConnect Secure Mobility Clients that connect to a FlexVPN server?

A. use of certificates instead of username and password
B. EAP-AnyConnect
C. EAP query-identity
D. AnyConnect profile

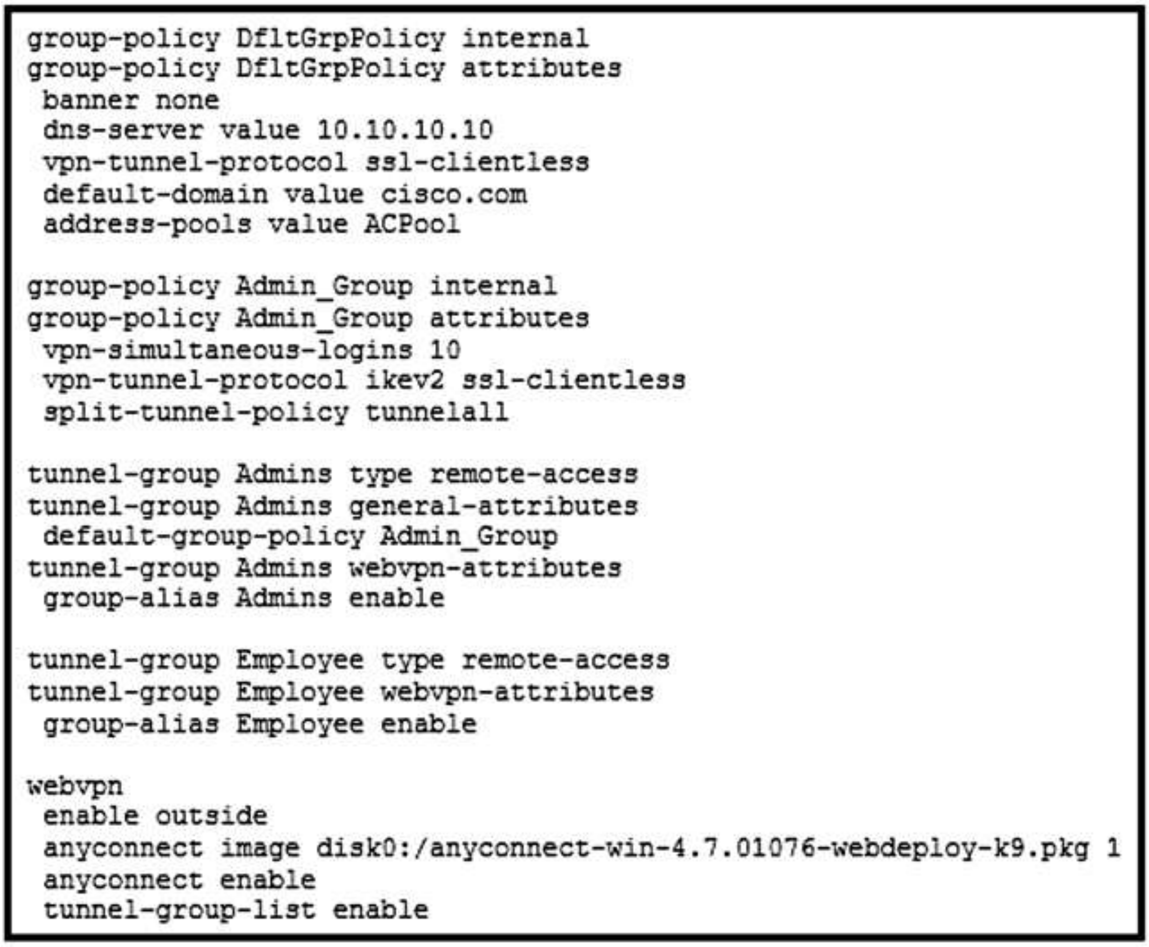
Answer: D
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

QUESTION 53
Which IKE identity does an IOS/IOS-XE headend expect to receive if an IPsec Cisco AnyConnect client uses default settings?

A. *$SecureMobilityClient$*
B. *$AnyConnectClient$*
C. *$RemoteAccessVpnClient$*
D. *$DfltIkeIdentityS*

Answer: B
Explanation:
https://www.cisco.com/c/en/us/support/docs/security/flexvpn/200555-FlexVPN-AnyConnect-IKEv2-Remote-Access.html

QUESTION 54
Refer to the exhibit. Which VPN technology is allowed for users connecting to the Employee tunnel group?



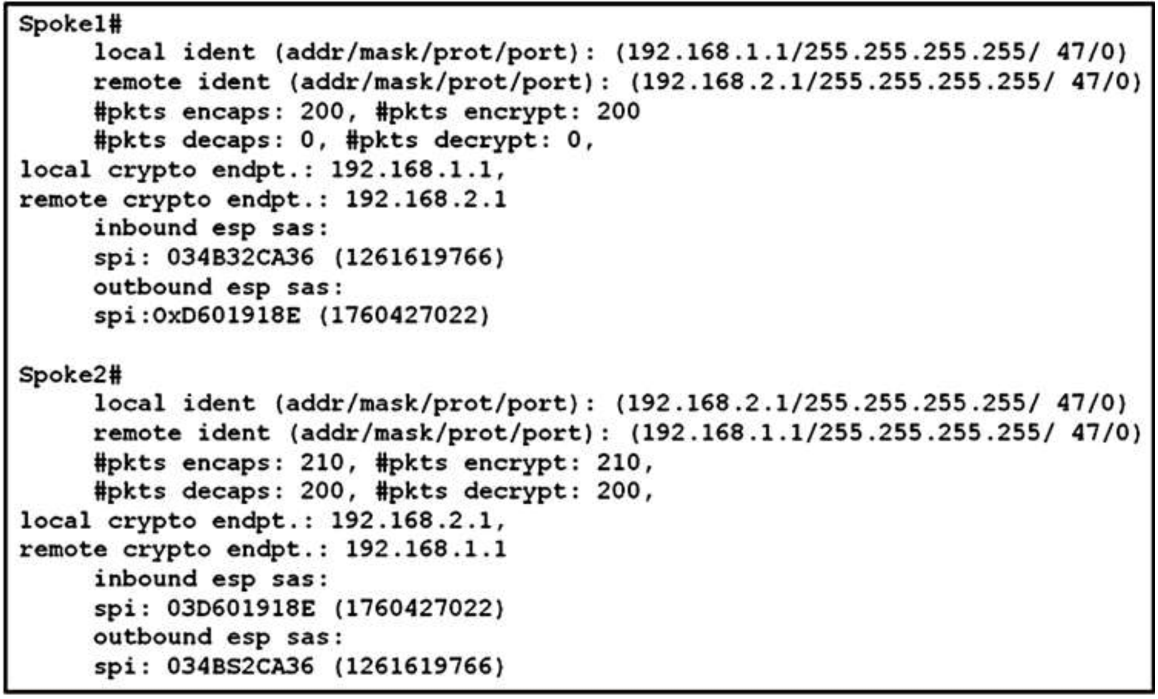
```
group-policy DfltGrpPolicy internal
group-policy DfltGrpPolicy attributes
 banner none
 dns-server value 10.10.10.10
 vpn-tunnel-protocol ssl-clientless
 default-domain value cisco.com
 address-pools value ACPool

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: B

QUESTION 55
Refer to the exhibit. An engineer is troubleshooting a new GRE over IPsec tunnel.
The tunnel is established but the engineer cannot ping from spoke 1 to spoke 2.
Which type of traffic is being blocked?



```
Spoke1#
     local ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     #pkts encaps: 200, #pkts encrypt: 200
     #pkts decaps: 0, #pkts decrypt: 0,
local crypto endpt.: 192.168.1.1,
remote crypto endpt.: 192.168.2.1
     inbound esp sas:
     spi: 034B32CA36 (1261619766)
     outbound esp sas:
     spi:0xD601918E (1760427022)

Spoke2#
     local ident (addr/mask/prot/port): (192.168.2.1/255.255.255.255/ 47/0)
     remote ident (addr/mask/prot/port): (192.168.1.1/255.255.255.255/ 47/0)
     #pkts encaps: 210, #pkts encrypt: 210,
     #pkts decaps: 200, #pkts decrypt: 200,
local crypto endpt.: 192.168.2.1,
remote crypto endpt.: 192.168.1.1
     inbound esp sas:
     spi: 03D601918E (1760427022)
     outbound esp sas:
     spi: 034BS2CA36 (1261619766)
```

A. ESP packets from spoke2 to spoke1
B. ISAKMP packets from spoke2 to spoke1
C. ESP packets from spoke1 to spoke2
D. ISAKMP packets from spoke1 to spoke2

Answer: A