Cisco

350-701 Exam

Implementing and Operating Cisco Security Core Technologies

Questions & Answers
Demo

Version: 14.0

Question: 1

What are two rootkit types? (Choose two)

A. registry
B. bootloader
C. buffer mode
D. user mode
E. virtual

Answer: B, D

Question: 2

When web policies are configured in Cisco Umbrella, what provides the ability to ensure that domains are blocked when they host malware, command and control, phishing, and more threats?

A. Application Control
B. Security Category Blocking
C. Content Category Blocking
D. File Analysis

Answer: B

Question: 3

An administrator is configuring a DHCP server to better secure their environment. They need to be able to rate-limit the traffic and ensure that legitimate requests are not dropped. How would this be accomplished?

A. Set a trusted interface for the DHCP server
B. Set the DHCP snooping bit to 1
C. Add entries in the DHCP snooping database
D. Enable ARP inspection for the required VLAN

Answer: A

Question: 4
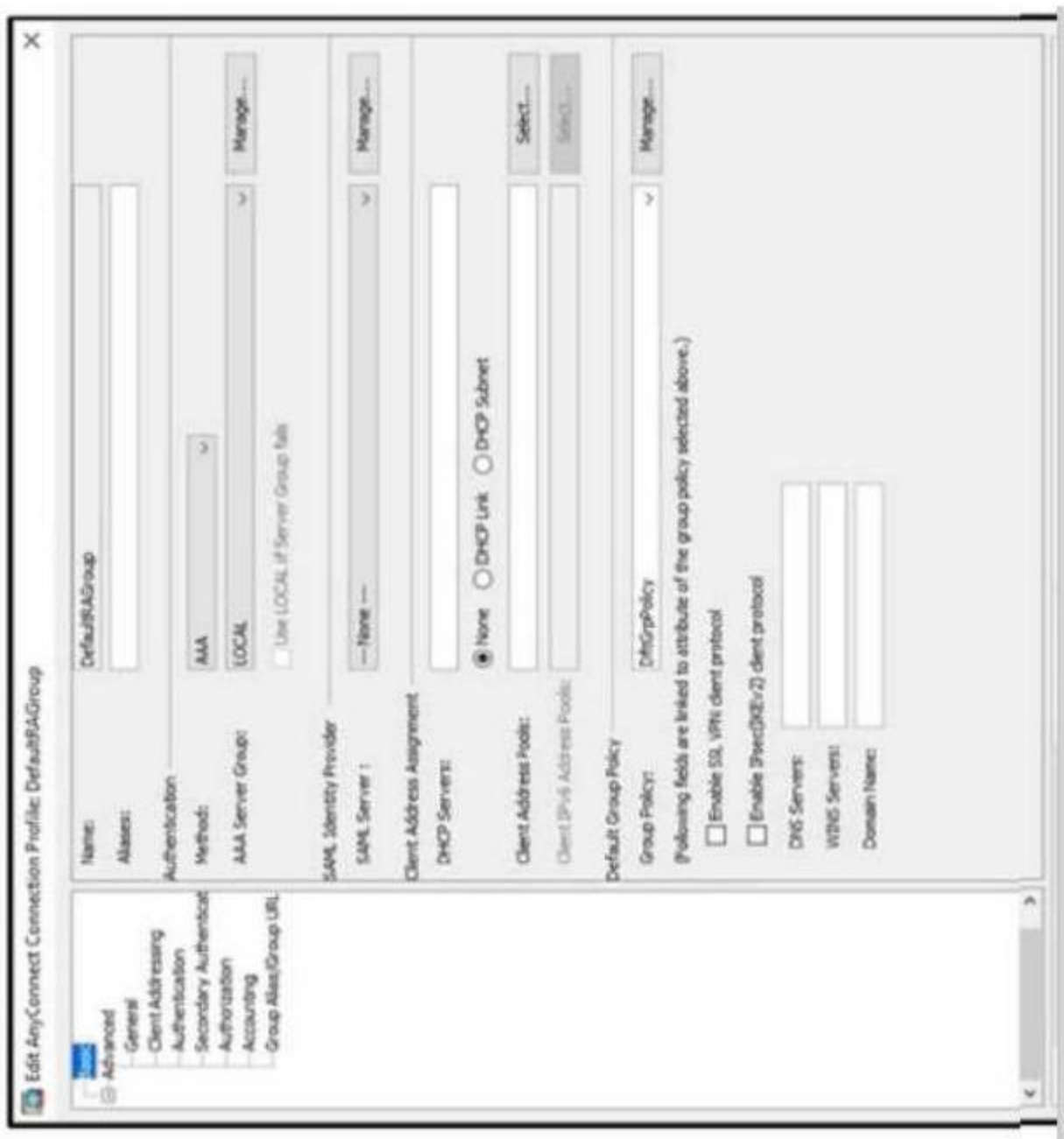
Refer to the exhibit. When configuring a remote access VPN solution terminating on the Cisco AS
A. an administrator would like to utilize an external token authentication mechanism in conjunction with
BA   authentication using machine certificates. Which configuration item must be modified to allow this?
A. Group policy
B. Method
C. SAML server
D. AAA server group

Answer: B

Question: 5

How is DNS tunneling used to exfiltrate data out of a corporate network?

A. It leverages the DNS server by permitting recursive lookups to spread the attack to other DNS servers.
B. lt encodes the payload with random characters that are broken into short strings and the DNS server rebuilds the exfiltrated data.
C. It redirects DNS requests to a malicious server used to steal user credentials, which allows further damage and theft on the network.
D. It corrupts DNS servers by replacing the actual IP address with a rogue address to collect information or start other attacks.

Answer: B