Cisco.500-470.v2025-05-15.q31

Exam Code:	500-470
Exam Name:	Cisco Enterprise Networks SDA, SDWAN and ISE Exam for System Engineers
Certification Provider:	Cisco
Free Question Number:	31
Version:	v2025-05-15
# of views:	699
# of Questions views:	310
https://www.exam-tests.com/500-470-exam/Cisco.500-470.v2025-05-15.q31.html	

NEW QUESTION: 1
Which are three functions used by ISE automation BYOD flow? (Choose three.)
A. Certificate Enrollment
B. Device Registration
C. BioMetrics
D. Active Directory Group Membership
E. LDAP Multi Tennant Provisioning
F. Supplicant Provisioning
Answer: (SHOW ANSWER)
Explanation
ISE automation BYOD flow is a process that allows users to self-enroll their devices to the network without requiring IT intervention. The process consists of three main functions: certificate enrollment, device registration, and supplicant provisioning.
Certificate enrollment is the function that allows users to obtain a digital certificate from a certificate authority (CA) for their devices. This certificate is used to authenticate the device to the network and provide secure communication. ISE supports different CA options, such as Microsoft CA, Cisco ISE CA, or third-party CA .
Device registration is the function that allows users to register their devices to the network and associate them with their identity. This enables ISE to apply policies based on the device type, ownership, and posture. ISE supports different device registration methods, such as portal-based, API-based, or bulk import .
Supplicant provisioning is the function that allows users to install and configure a network access client (supplicant) on their devices. This client is used to connect to the network using the appropriate protocols and settings. ISE supports different supplicant provisioning methods, such

as native supplicant, Cisco Network Setup Assistant (NSA), or Cisco AnyConnect Secure Mobility Client (AnyConnect) .
References:
[Cisco Identity Services Engine Administrator Guide, Release 2.7 - BYOD [Cisco Identity Services Engine]] :
[Cisco Identity Services Engine Administrator Guide, Release 2.7 - Certificate Provisioning [Cisco Identity Services Engine]] : [Cisco Identity Services Engine Administrator Guide, Release 2.7 - Device Registration
[Cisco Identity Services Engine]] : [Cisco Identity Services Engine Administrator Guide, Release 2.7 - Supplicant Provisioning [Cisco Identity Services Engine]]

NEW QUESTION: 2
Which are three Cisco recommendations on "How to Win"? (Choose three.)
A. Show case Cisco portfolio or ISE feature set during PoC
B. Demonstrate complex policy flows, rather show case Wizards and enhanced context visibility.
C. Talk about Cisco's focus on Security and integration with StealthWatch, Sourcefire, WSA, vulnerability scanner to make smarter policy decisions.
D. Explain architectural advantage of holistic Cisco solution.
E. Explain support for 3rd party network devices.
Answer: A,C,D (LEAVE A REPLY)

NEW QUESTION: 3
How many vEdge router security zones (VPN's) can be configured?
A. 510
B. 32
C. 256
D. 16
Answer: A (LEAVE A REPLY)
Explanation
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.1/04Segmentation/02Conf

NEW QUESTION: 4
What is the role of DNA Center in SD-Access?
A. provide GUI management abstraction & Analytics via Multiple Service Apps
B. Identifying and Authenticating Endpoints
C. The point of exchange of reachability and policy for two domains
D. Maintain a database of Endpoint IDs to Fabric Edge Nodes
Answer: A (LEAVE A REPLY)

NEW QUESTION: 5

Which two options are SD-WAN solution capabilities? (Choose two.)
A. Cloud hosted or on-Premise fully redundant management and control plane functions
B. Ability to provide and integrate security with complementary products and applications
C. The separation of management plane, control plane and data plane to enable horizontal scaling
D. Truck roll branch turn up for easy provisioning and new installations
Answer: A,C (LEAVE A REPLY)

NEW QUESTION: 6
Which two options are SD-WAN solution capabilities? (Choose two.)
A. Trust roll branch turn up for easy provisioning and new installations
B. The separation of management plane, control plane and data plane to enable horizontal scaling
C. Cloud hosted or on-Premise fully redundant management and control plane functions
D. Ability to provide and integrate security with complementary products and applications
Answer: B,C (LEAVE A REPLY)
Explanation
SD-WAN is a software-defined approach to managing the WAN that offers several capabilities, such as:
The separation of management plane, control plane and data plane to enable horizontal scaling. This means that the SD-WAN solution can decouple the network functions from the underlying hardware and distribute them across different layers and locations. This allows for greater flexibility, scalability, and resilience of the network12 Cloud hosted or on-premise fully redundant management and control plane functions. This means that the SD-WAN solution can provide centralized and cloud-based management and control of the network, as well as the option to deploy them on-premise for more control and security. This enables the SD-WAN solution to offer consistent policies, visibility, and analytics across the network, as well as the ability to automate network operations and orchestration13 The other options are not SD-WAN solution capabilities, but rather features or benefits of specific SD-WAN solutions, such as:
Trust roll branch turn up for easy provisioning and new installations. This is a feature of Cisco Catalyst SD-WAN, which enables zero-touch provisioning and automated configuration of branch devices, as well as the ability to trust the identity and security posture of the devices3 Ability to provide and integrate security with complementary products and applications. This is a benefit of Cisco Catalyst SD-WAN, which offers integrated security capabilities, such as full-stack multilayer security, cloud-delivered security, and SASE-enabled architecture. This enables the SD-WAN solution to provide real-time threat protection and compliance across the network3 References := What Is SD-WAN? - Software-Defined WAN (SDWAN) - Cisco SD-WAN Solution - Cisco Catalyst SD-WAN Solution Overview What is SD-WAN? - Software-Defined WAN | VMware

NEW QUESTION: 7
What is an example of Correlated Insights for SDA and Switching?
A. Excessive Onboarding Time
B. Roaming Pattern Analysis

C. Control Plane Reachability
D. AP License Utilization
Answer: C (LEAVE A REPLY)
Explanation/Reference:
Reference: http://www.tyrc.edu.tw/images/2/29/107051006.pdf page 72

NEW QUESTION: 8
Which two options are used as part of an ISE POV? (Choose two.)
A. Implementation on Production Network
B. POV Kit
C. Youtube
D. dCloud
E. CiscoTV
Answer: B,D (LEAVE A REPLY)

NEW QUESTION: 9
Which three options describe fabric overlay concepts? (Choose three.)
A. Intermediate System to Intermediate System
B. A virtual Local Area Network
C. An Overlay is a logical topology
D. GRE is a type of Overlay
E. A link state routing protocol like OSPF
F. An Overlay uses alternate forwarding attributes
Answer: (SHOW ANSWER)
Explanation
Fabric overlay concepts are related to the creation of a virtual network topology on top of a physical network infrastructure. The overlay network is usually designed to provide services or features that are not directly supported by the underlay network, such as network segmentation, mobility, or security. Some of the fabric overlay concepts are:
An overlay is a logical topology: An overlay network is a network that is built on top of another network using software or hardware devices that encapsulate and decapsulate packets. The overlay network creates a logical topology that is independent of the physical topology of the underlay network. The overlay network can span multiple Layer 2 or Layer 3 domains and provide end-to-end connectivity for the overlay endpoints. An example of an overlay network is a VPN that connects remote sites over the Internet.
GRE is a type of overlay: Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets of one protocol type within another protocol type. GRE is used to create tunnels between devices that can carry different types of traffic, such as IP, IPv6, MPLS, or Ethernet. GRE is a type of overlay network that can be used to extend Layer 2 or Layer 3 connectivity across different networks or to provide a secure and private communication channel. An example of a GRE

overlay network is a DMVPN that uses GRE tunnels to connect branch offices to a central hub over the Internet.
An overlay uses alternate forwarding attributes: An overlay network uses different attributes or identifiers to forward packets than the underlay network. The overlay network adds specific headers or tags to the packets that contain information about the overlay endpoints, such as their logical addresses, group memberships, or policies. The overlay devices use these attributes to forward packets based on the overlay topology and services, rather than the underlay topology and protocols. The underlay devices are unaware of the overlay attributes and forward packets based on the underlay headers. An example of an overlay network that uses alternate forwarding attributes is a VXLAN network that uses VNIs to segment traffic and provide Layer 2 connectivity over a Layer 3 network.
The other options, Intermediate System to Intermediate System (IS-IS), a virtual Local Area Network (VLAN), and a link state routing protocol like OSPF, are not fabric overlay concepts. IS-IS and OSPF are routing protocols that are used to exchange routing information and build the routing table of the underlay network. A VLAN is a Layer 2 segmentation technique that divides a physical network into logical subnets based on the switch port membership. A VLAN is not an overlay network, but it can be part of the underlay network or the overlay network, depending on the design. References := : Fabric Technologies and Overlays - Cisco Learning Network1, What Is a Network Fabric? - Cisco2

NEW QUESTION: 10
Which is a key function of a Digital Network?
A. Centralized provisioning
B. Provides secure data plane with remote vEdge routers
C. Nat traversal
D. Software upgrades
Answer: (SHOW ANSWER)
Explanation
A Digital Network is a network that is based on the Cisco Digital Network Architecture (Cisco DNA), which is an open and extensible, software-driven network architecture designed to rapidly deliver services that enable IT to innovate faster, reduce costs and complexity, lower risk, and comply with regulatory requirements1. A key function of a Digital Network is centralized provisioning, which allows IT to automate the deployment and configuration of network devices and services using a single platform, such as the Cisco DNA Center2.
Centralized provisioning simplifies network management, reduces human errors, and accelerates network changes.
References:
2: [Cisco DNA Software - Digital Network Architecture - Cisco] : 1: [Cisco Digital Network Architecture]

NEW QUESTION: 11

Which protocol is used between an Endpoint and a Switch with an 802.1 authentication?
A. TACACS
B. EAP
C. RADIUS
D. MAB
Answer: B (LEAVE A REPLY)

NEW QUESTION: 12
How many bytes does a VxLAN header add to an original Ethernet frame?
A. 50
B. 48
C. 64
D. 36
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
Which two products are supported as "Extended" in DNA-C 1.1? (Choose two.)
A. IE switches
B. Catalyst 6807
C. Catalyst 3560-CX
D. M3 Line cards
E. AP 3800
F. Catalyst 4500-E
Answer: (SHOW ANSWER)
Explanation/Reference:
Reference: https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/software-defined- access/guide-c07-739242.pdf

NEW QUESTION: 14
Which are three Cisco recommendations on "How to Win"? (Choose three.)
A. Explain support for 3rd party network devices.
B. Show case Cisco portfolio or ISE feature set during PoC.
C. Explain architectural advantage of holistic Cisco solution.
D. Talk about Cisco's focus on Security and integration with StealthWatch, Sourcefire, WSA, vulnerability scanner to make smarter policy decisions
E. Demonstrate complex policy flows, rather show case Wizards and enhanced context visibility.
Answer: A,C,D (LEAVE A REPLY)
Explanation
According to the Cisco Enterprise Networks SDA, SDWAN and ISE Exam for System Engineers document1, the three Cisco recommendations on "How to Win" are:

Explain support for 3rd party network devices: Cisco ISE can integrate with more than 60 third-party solutions that span across security and network portfolios. This enablesCisco ISE to leverage the information and capabilities of these solutions to enhance the identity and access management, network visibility and segmentation, threat detection and response, and policy enforcement of the network. By explaining this support, the customer can see the value and flexibility of Cisco ISE in their existing or heterogeneous network environment2.
Explain architectural advantage of holistic Cisco solution: Cisco ISE is part of the Cisco Digital Network Architecture (DNA), which is a comprehensive and open platform that provides end-to-end network automation, assurance, security, and analytics. By explaining the architectural advantage of the holistic Cisco solution, the customer can see how Cisco ISE works seamlessly with other Cisco DNA components, such as Cisco DNA Center, Cisco SD-Access, Cisco SD-WAN, Cisco TrustSec, and Cisco Stealthwatch, to deliver a unified and consistent network experience across wired, wireless, and cloud domains3.
Talk about Cisco's focus on Security and integration with StealthWatch, Sourcefire, WSA, vulnerability scanner to make smarter policy decisions: Cisco ISE is a core component of the Cisco security portfolio, which provides comprehensive and integrated security solutions for the network. By talking about Cisco's focus on security and integration with other security products, such as StealthWatch, Sourcefire, WSA, and vulnerability scanner, the customer can see how Cisco ISE can provide enhanced visibility, threat detection, and policy enforcement for the network. For example, Cisco ISE can use the data from StealthWatch to identify anomalous or malicious behavior of the endpoints and apply appropriate network access policies based on the threat level4.
The other options, show case Cisco portfolio or ISE feature set during PoC and demonstrate complex policy flows, rather show case Wizards and enhanced context visibility, are not Cisco recommendations on "How to Win". Showing case Cisco portfolio or ISE feature set during PoC is a general best practice, but not a specific recommendation for winning the customer. Demonstrating complex policy flows, rather than showing case Wizards and enhanced context visibility, is a counterproductive approach, as it can confuse or overwhelm the customer with technical details, rather than highlighting the benefits and simplicity of Cisco ISE. References := : 2: Cisco Identity Services Engine Administrator Guide, Release 2.7 - ISE Security Ecosystem Integration Guides [Cisco Identity Services Engine] - Cisco2, 1: Cisco Enterprise Networks SDA, SDWAN and ISE Exam for System Engineers1, 3: Cisco Identity Services Engine - Cisco3, 4: Cisco Identity Services Engine Administrator Guide, Release 2.7 - Stealthwatch Integration [Cisco Identity Services Engine] - Cisco4

NEW QUESTION: 15
Which three wireless product families are supported in the current DNA-C 1.1 release? (Choose three.)
A. WLC 5508
B. WLC 8540
C. WLC 3504

D. AP 1260
E. AP 3800
Answer: B,C,E (LEAVE A REPLY)

NEW QUESTION: 16
Which three statements best describe Cisco ISE configuration capabilities? (Choose three.)
A. ISE Deployment Assistant (IDA) is a built in application designed to accelerate the deployment of Cisco Identity Service Engine (ISE)
B. ISE wizards and pre-canned configurations ease ISE roll-out significantly.
C. ISE requires an understanding of the command line for set-up and configuration.
D. Cisco Active Advisor provides additional guidance for ISE deployments
E. Cisco ISE includes wireless setup wizard and visibility wizard.
Answer: A,D,E (LEAVE A REPLY)

NEW QUESTION: 17
Which three services must be enabled under the ISE Admin settings to successfully integrate ISE, when integrating ISE with DNA-C? (Choose three.)
A. PxGrid
B. ServiceNow
C. SXP services
D. Threat- Centric NAC
E. Passive Identity Service
F. Infoblox
Answer: A,C,E (LEAVE A REPLY)

NEW QUESTION: 18
Which Cisco SD WAN component provides a secure data plane with remote vEdge routers?
A. vBond
B. vSmart
C. vManage
D. vEdge
Answer: D (LEAVE A REPLY)

Explanation
https://sdwan-docs.cisco.com/Product_Documentation/Software_Features/Release_18.2/05Security/01Security_Overview/Data_Plane_Security_Overview vEdge is the Cisco SD WAN component that provides a secure data plane with remote vEdge routers. vEdge routers are the devices that sit at the edge of the SD WAN fabric and connect to the WAN transports, such as MPLS, Internet, or LTE. vEdge routers establish secure IPsec tunnels with other vEdge routers in the fabric and exchange routing and policy information with the vSmart controller. vEdge routers also perform application-aware routing, QoS, and security functions on the data plane traffic. vEdge routers can be physical or virtual devices and can be deployed in branch, campus, data center, or cloud environments1.
The other options, vBond, vSmart, and vManage, are not the components that provide a secure data plane with remote vEdge routers. vBond is the orchestrator that performs the initial authentication and authorization of vEdge routers and assigns them to a vSmart controller. vSmart is the controller that distributes the control and data policies and the network topology information to the vEdge routers. vManage is the management platform that provides centralized configuration, monitoring, and troubleshooting of the SD WAN fabric1.
References := : 1: Cisco SD-WAN Getting Started Guide - Cisco SD-WAN Overview [Cisco SD-WAN] - Cisco

NEW QUESTION: 19
Which protocol is used between an Endpoint and a Switch with an 802.1 authentication?
A. TACACS
B. EAP
C. MAB
D. RADIUS
Answer: B (LEAVE A REPLY)
Explanation
https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3750/software/release/15-0_2_se/configuration/guide/scg3750/sw8021x.pdf
The protocol that is used between an endpoint and a switch with an 802.1 authentication is EAP, which stands for Extensible Authentication Protocol. EAP is a framework that defines how the endpoint (also called the supplicant) and the switch (also called the authenticator) exchange authentication messages over a wired or wireless network. EAP supports various authentication methods, such as passwords, certificates, tokens, or biometrics, and can be encapsulated in different transport protocols, such as RADIUS, Diameter, or EAPOL. EAP is used in 802.1X authentication, which is a standard for port-based network access control that prevents unauthorized access to a network1.
The other options, TACACS, MAB, and RADIUS, are not protocols that are used between an endpoint and a switch with an 802.1 authentication. TACACS is a protocol that provides remote authentication and authorization for network devices, such as routers or switches, but it is not used for endpoint authentication.

MAB is a technique that uses the MAC address of an endpoint as a credential for 802.1X authentication, but it is not a protocol itself. RADIUS is a protocol that provides centralized authentication, authorization, and accounting for network access, but it is not used directly between the endpoint and the switch, but rather between the switch and the authentication server1. References := : 2: What Is 802.1X Authentication? How Does 802.1x Work? - Fortinet2, 1: IEEE 802.1X - Wikipedia1

NEW QUESTION: 20
What is a challenge of having an SD-Access Centralized design where a single fabric encompasses the main site and all branch sites across the WAN?
A. DNA Center does not support it
B. SSIDs would be the same across all sites
C. Since the traffic is encapsulated. SD-WAN features can't be used to optimize/route traffic.
D. End to End Routing is not supported
Answer: (SHOW ANSWER)

NEW QUESTION: 21
Which options are Network Access Device types?
A. Switches, Wireless Controllers, and Routers
B. Switches, Routers, and VPN Gateways
C. Switches, Wireless Controllers, and VPN Gateways
D. Wireless Controllers, Routers, and VPN Gateways
Answer: C (LEAVE A REPLY)

NEW QUESTION: 22
Which three statements best describe Cisco ISE configuration capabilities? (Choose three.)
A. Cisco ISE includes wireless setup wizard and visibility wizard.
B. ISE Deployment Assistant (IDA) is a built in application designed to accelerate the deployment of Cisco Identity Service Engine (ISE)
C. ISE wizards and pre-canned configurations ease ISE roll-out significantly.
D. ISE requires an understanding of the command line for set-up and configuration.
E. Cisco Active Advisor provides additional guidance for ISE deployments
Answer: (SHOW ANSWER)

NEW QUESTION: 23
How many vEdge router security zones (VPN's) can be configured?
A. 16
B. 32
C. 256
D. 510
Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
Where does the Cisco V-Edge Router perform QOS traffic classification?
A. Egress interface
B. Per vEdge
C. Per VPN
D. Ingress interface
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which options are Network Access Device types?
A. Switches, Wireless Controllers, and Routers
B. Switches, Routers, and VPN Gateways
C. Switches, Wireless Controllers, and VPN Gateways
D. Wireless Controllers, Routers, and VPN Gateways
Answer: C (LEAVE A REPLY)
Explanation
https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/Campus/CVD-Software-Defined-Access-Design-Gu References := Some possible references are:
Cisco Enterprise Networks SDA, SDWAN and ISE Exam for System Engineers (ENSDENG) Study Guide Cisco Identity Services Engine Administrator Guide, Release 2.7 - Configure Network Access Devices
[Cisco Identity Services Engine]

NEW QUESTION: 26
What two best describe self-healing functionality on vEdges? (Choose two.)
A. vManage detect routing outage detection to detect reachability outages and understand their scope and likely root cause
B. With configuration change, rolling back the configuration change when loss of connectivity to vManage
C. In software upgrade process, rolling back to the previously running software image when connectivity to vManage fails
D. Software reconfiguration capability allowing for dynamic reconfiguration of existing channels
Answer: B,C (LEAVE A REPLY)

NEW QUESTION: 27
Which party solution integrates with Cisco's security and network portfolios within the ISE?
A. 30+ 3rd party solutions
B. 60+ 3rd party solutions
C. 20+ 3rd party solutions
D. 45+ 3rd party solutions

E. 25+ 3rd party solutions

Answer: B (LEAVE A REPLY)

Explanation

Cisco ISE integrates with more than 60 third-party solutions that span across security and network portfolios.

These solutions include network access devices, firewalls, threat detection and prevention systems, vulnerability scanners, endpoint management platforms, cloud services, and more. By integrating with these solutions, Cisco ISE can leverage the information and capabilities of these solutions to enhance the identity and access management, network visibility and segmentation, threat detection and response, and policy enforcement of the network. Some of the examples of third-party solutions that integrate with Cisco ISE are:

Fortinet: Fortinet integrates with Cisco ISE through pxGrid to share user and device information, security group tags, and endpoint posture status. This enables Fortinet to apply granular and dynamic firewall policies based on the identity and context of the endpoints1.

Tripwire: Tripwire integrates with Cisco ISE through pxGrid to share vulnerability and compliance data of the endpoints. This enables Cisco ISE to apply appropriate network access policies based on the risk and compliance level of the endpoints2.

Splunk: Splunk integrates with Cisco ISE through REST APIs to collect and analyze the logs and events generated by Cisco ISE. This enables Splunk to provide network and security insights, dashboards, reports, and alerts based on the Cisco ISE data3.

References := : Cisco Identity Services Engine Administrator Guide, Release 2.7 - ISE Security Ecosystem Integration Guides [Cisco Identity Services Engine] - Cisco4, Solved: ISE Integration with 3rd party solution - Cisco Community1, ISE Security Ecosystem Integration Guides - Cisco Community5, Cisco Identity Services Engine Administrator Guide, Release 2.7 - Splunk Integration [Cisco Identity Services Engine] - Cisco3, Cisco Identity Services Engine Administrator Guide, Release 2.7 - Tripwire Integration [Cisco Identity Services Engine] - Cisco2 https://www.ciscolive.com/c/dam/r/ciscolive/apjc/docs/2017/pdf/BRKSEC-2141.pdf slide 9

NEW QUESTION: 28

Which are three Cisco recommendations on "How to Win"? (Choose three.)

A. Demonstrate complex policy flows, rather show case Wizards and enhanced context visibility.

B. Explain support for 3rd party network devices.

C. Show case Cisco portfolio or ISE feature set during PoC

D. Explain architectural advantage of holistic Cisco solution.

E. Talk about Cisco's focus on Security and integration with StealthWatch, Sourcefire, WSA, vulnerability scanner to make smarter policy decisions.

Answer: (SHOW ANSWER)

NEW QUESTION: 29

Which two products are supported as "Extended" in DNA-C 1.1? (Choose two.)

A. Catalyst 3560-CX

B. M3 Line cards
C. Catalyst 4500-E
D. IE switches
E. Catalyst 6807
F. AP 3800
Answer: A,D (LEAVE A REPLY)
Explanation
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/software-defined-access/guide-c07-7

NEW QUESTION: 30
Which three statements are true regarding Cisco SDWAN license tiers? (Choose three.)
A. With Pro license, control and data policies are supported
B. With Plus license, split-tunnel is supported
C. With Pro license, unlimited segmentations are supported
D. With Plus license, Hub and spoke, partial mesh are supported
E. With Enterprise license, vAnalytics is included
F. With Enterprise license, TCP optimization is not supported
Answer: A,B,E (LEAVE A REPLY)
Explanation
Some of the statements that are true regarding Cisco SD-WAN license tiers are:
With Pro license, control and data policies are supported2. This license tier enables network operators to define and enforce policies for traffic shaping, quality of service (QoS), application optimization, and security2.
With Plus license, split-tunnel is supported3. This license tier enables network operators to use split-tunneling technology to route traffic through different paths based on application or user preferences3.
With Enterprise license, vAnalytics is included4. This license tier enables network operators to use vAnalytics feature to collect and analyze data from various sources such as endpoints, applications, devices, networks, and cloud services4.

NEW QUESTION: 31
How does identity management solve two customer problems? (Choose two.)
A. Enables and enforces 802.1X across the network platform
B. Increases digitization
C. Achieves dynamic and adaptive network segmentation
D. Provides network visibility and security
E. Manages group membership
Answer: (SHOW ANSWER)

Valid 500-470 Dumps shared by BraindumpsPass.com for Helping Passing 500-470 Exam! BraindumpsPass.com now offer the **newest 500-470 exam dumps**, the BraindumpsPass.com 500-470 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 500-470 dumps with Test Engine here: https://www.braindumpspass.com/Cisco/500-470-practice-exam-dumps.html (**38** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

Valid 500-470 Dumps shared by BraindumpsPass.com for Helping Passing 500-470 Exam! BraindumpsPass.com now offer the **newest 500-470 exam dumps**, the BraindumpsPass.com 500-470 exam **questions have been updated** and **answers have been corrected** get the **newest** BraindumpsPass.com 500-470 dumps with Test Engine here: https://www.braindumpspass.com/Cisco/500-470-practice-exam-dumps.html (**38** Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)