Latest sce_sles_15 Visual Cert Exam - Find Shortcut to Pass sce_sles_15 Exam - Everbrasil

We would appreciate if you can choose our sce_sles_15 training material, Now you need not be worried, if you are run short of time for sce_sles_15 exam preparation or your tough work schedule doesn't allow you spare time for studying preparatory guides, When it comes to our SUSE Certified Engineer (SCE) in Enterprise Linux sce_sles_15 exam dumps, we are confident that the quality and validity are incomparable, which can help you pass the sce_sles_15 exam test with ease, Also download sce_sles_15SUSE Certified Engineer in Enterprise Linux 15 SUSE online demo practice test before purchasing sce_sles_15 online practice questions and answers.

Download Case Studies related to this title, Department of New CDMS-SMM3.0 Test Vce Free Justice over allegations of monopolistic practices, Multivoltage Power Supplies, Then we created a storyline.

One option is to use Remote Desktop to schedule computers to **sce_sles_15 Exam Fee** power on over the weekend or at night and then power off, leaving a window of time for them all to transmit report data.

Youll learn how to manage data breaches as the true **sce_sles_15 Exam Fee** crises they are, When the truth becomes certain and this certainty evokes from its essence the fundamental properties of its basic nature, the comprehensive **sce_sles_15 Exam Fee** guarantee of a structure based on a particular self-assurance, reality becomes its own essence.

No need to spend a lot of time and money while youâ€™ve access to sce_sles_15 exam dumps, So what's the difference between a sweepstakes and a lottery, Follow the instructions to download this book's companion file.
 sce_sles_15 Exam Fee - Successfully Pass The SUSE Certified Engineer in Enterprise Linux 15
We would appreciate if you can choose our sce_sles_15 training material, Now you need not be worried, if you are run short of time for sce_sles_15 exam preparation or your tough work schedule doesn't allow you spare time for studying preparatory guides.

When it comes to our SUSE Certified Engineer (SCE) in Enterprise Linux sce_sles_15 exam dumps, we are confident that the quality and validity are incomparable, which can help you pass the sce_sles_15 exam test with ease.

Also download sce_sles_15SUSE Certified Engineer in Enterprise Linux 15 SUSE online demo practice test before purchasing sce_sles_15 online practice questions and answers, Before purchasing our SUSE Certified Engineer in Enterprise Linux 15

practice materials, you can have a thoroughly view of demos for experimental trial, and **sce_sles_15 Exam Fee** once you decided to get them, which is exactly a sensible choice, you can obtain them within ten minutes without waiting problems.

Here we offer the most useful sce_sles_15 practice test for your reference, And we keep updating our sce_sles_15 learing quiz all the time, If you wonder the sce_sles_15 valid exam materials for IT certification exam is accurate and valid you can rest assured.
Updated sce_sles_15 Practice Exam Questions
If you pass multiple packaging s, you will be exposed to the global business sce_sles_15 opportunities in the job market, With our SUSE Certified Engineer in Enterprise Linux 15 useful pdf files, you can prepare and practice in a comprehensive and systematic way.

Everbrasil sce_sles_15 dumps pdf includes a number of questions and answers for the practice of the SUSE Certified Engineer (SCE) in Enterprise Linux students that will not only provide the questions for sce_sles_15 exam but will also prepare his mind and build confidence for the real SUSE Certified Engineer in Enterprise Linux 15 exam.

Our sce_sles_15 dumps are better than all other cheap sce_sles_15 study material, We made it by persistence, patient and enthusiastic as well as responsibility, You need Avanset VCE Exam Simulator in order to study the SUSE SUSE Certified Engineer (SCE) in Enterprise Linux sce_sles_15 exam dumps & practice test questions.

Because this exam is difficult, through it, you may be subject SUSE Certified Engineer in Enterprise Linux 15 to international recognition and acceptance, and you will have a bright future and holding high pay attention.

If there is something new, we will send it to your email immediately, If you're doubtful about the excellence of sce_sles_15 exam material, so you may try the free demo to test the quality features of our material.

If you study with our sce_sles_15 exam questions, then you will be surprised to find that our sce_sles_15 training material is well-written and excellently-organised.

We have professional technicians to exam the website every day, PL-400 Visual Cert Exam therefore the safety for the website can be guaranteed, Don't let the trifles be a drag on your career development.

NEW QUESTION: 1
Which option describes the Network Security feature of Cisco intergrated Management Controller?

A. A feature that locks users out of the Cisco IMC after a specified number of unsuccessful log in attempts.
B. A list that specifies the devices allowed to access the Cisco IMC.
C. User-configured ACLs that deny devices access to the Cisco IMC.
D. 802.1x support which permits the Cisco IMC access to the port security network.
Answer: A

NEW QUESTION: 2
DRAG DROP
Select and Place:

Answer:
Explanation:

Explanation/Reference:
IPv6-in-IPv4 and GRE are manual and 6RDand 6to4

Download this chapter
Implementing Tunnels
Download the complete book
Interface and Hardware Component Configuration Guide, Cisco IOS XE Release 3S (PDF - 1 MB) Feedback
Contents
Implementing Tunnels
Finding Feature Information
Restrictions for Implementing Tunnels
Information About Implementing Tunnels
Tunneling Versus Encapsulation
Tunnel ToS
Generic Routing Encapsulation
GRE Tunnel IP Source and Destination VRF Membership
GRE IPv4 Tunnel Support for IPv6 Traffic
EoMPLS over GRE
Provider Edge to Provider Edge Generic Routing EncapsulationTunnels
Provider to Provider Generic Routing Encapsulation Tunnels
Provider Edge to Provider Generic Routing Encapsulation Tunnels
Features Specific to Generic Routing Encapsulation
Features Specific to Ethernet over MPLS
Features Specific to Multiprotocol Label Switching Virtual Private Network Overlay Tunnels for IPv6
IPv6 Manually Configured Tunnels
Automatic 6to4 Tunnels
ISATAP Tunnels
Path MTU Discovery
QoS Options for Tunnels
How to Implement Tunnels
Determining the Tunnel Type

Implementing Tunnels

Last Updated: September 17, 2012

This module describes the various types of tunneling techniques. Configuration details and examples are provided for the tunnel types that use physical or virtual interfaces. Many tunneling techniques are implemented using technology-specific commands, and links are provided to the appropriate technology modules.

Tunneling provides a way to encapsulate arbitrary packets inside a transport protocol. Tunnels are implemented as virtual interfaces to provide a simple interface for configuration purposes. The tunnel interface is not tied to specific "passenger" or "transport" protocols, but rather is an architecture to provide the services necessary to implement any standard point-to-point encapsulation scheme.

Note

Cisco ASR 1000 Series Aggregation Services Routers support VPN routing and forwarding (VRF)-aware generic routing encapsulation (GRE) tunnel keepalive features.

Finding Feature Information

Your software release may not support all the features

documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support.
To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.
Restrictions for Implementing Tunnels
It is important to allow the tunnel protocol to pass through a firewall and access control list (ACL) check.
Multiple point-to-point tunnels can saturate the physical link with routing information if the bandwidth is not configured correctly on a tunnel interface.
A tunnel looks like a single hop link, and routing protocols may prefer a tunnel over a multihop physical path.
The tunnel, despite looking like a single hop link, may traverse a slower path than a multihop link. A tunnel is as robust and fast, or as unreliable and slow, as the links that it actually traverses. Routing protocols that make their decisions based only on hop counts will often prefer a tunnel over a set of physical links. A tunnel might appear to be a one-hop, point-to-point link and have the lowest-cost path, but the tunnel may actually cost more in terms of latency when compared to an alternative physical topology. For example, in the topology shown in the figure below, packets from Host 1 will appear to travel across networks w, t, and z to get to Host 2 instead of taking the path w, x, y, and z because the tunnel hop count appears shorter. In fact, the packets going through the tunnel will still be traveling across Router A, B, and C, but they must also travel to Router D before coming back to Router C.
Figure 1
Tunnel Precautions: Hop Counts
A tunnel may have a recursive routing problem if routing is not configured accurately. The best path to a tunnel destination is via the tunnel itself; therefore recursive routing causes the tunnel interface to flap. To avoid recursive routing problems, keep the control-plane routing separate from the tunnel routing by using the following methods:
Use a different autonomous system number or tag.
Use a different routing protocol.
Ensure that static routes are used to override the first hop (watch for routing loops).
The following error is displayed when there is recursive routing to a tunnel destination:
%TUN-RECURDOWN Interface Tunnel 0
temporarily disabled due to recursive routing
Information About Implementing Tunnels
Tunneling Versus Encapsulation
Tunnel ToS

Generic Routing Encapsulation
EoMPLS over GRE
Overlay Tunnels for IPv6
IPv6 Manually Configured Tunnels
Automatic 6to4 Tunnels
ISATAP Tunnels
Path MTU Discovery
QoS Options for Tunnels
Tunneling Versus Encapsulation
To understand how tunnels work, you must be able to distinguish between concepts of encapsulation and tunneling. Encapsulation is the process of adding headers to data at each layer of a particular protocol stack.
The Open Systems Interconnection (OSI) reference model describes the functions of a network. To send a data packet from one host (for example, a PC) to another on a network, encapsulation is used to add a header in front of the data packet at each layer of the protocol stack in descending order. The header must contain a data field that indicates the type of data encapsulated at the layer immediately above the current layer. As the packet ascends the protocol stack on the receiving side of the network, each encapsulation header is removed in reverse order.
Tunneling encapsulates data packets from one protocol within a different protocol and transports the packets on a foreign network. Unlike encapsulation, tunneling allows a lower-layer protocol and a same- layer protocol to be carried through the tunnel. A tunnel interface is a virtual (or logical) interface.
Tunneling consists of three main components:
Passenger protocol--The protocol that you are encapsulating. For example, IPv4 and IPv6 protocols.
Carrier protocol--The protocol that encapsulates. For example, generic routing encapsulation (GRE) and Multiprotocol Label Switching (MPLS).
Transport protocol--The protocol that carries the encapsulated protocol. The main transport protocol is IP.
The figure below illustrates IP tunneling terminology and concepts:
Figure 2
IP Tunneling Terminology and Concepts
Tunnel ToS
Tunnel type of service (ToS) allows you to tunnel network traffic and group all packets in the same ToS byte value. The ToS byte values and Time-to-Live (TTL) hop-count value can be set in the encapsulating IP header of tunnel packets for an IP tunnel interface on a router. Tunnel ToS feature is supported for Cisco Express Forwarding (formerly known as CEF), fast switching, and process switching.
The ToS and TTL byte values are defined in RFC 791. RFC 2474, and RFC 2780 obsolete the use of the ToS byte as defined in RFC 791. RFC 791 specifies that bits 6 and 7 of the ToS byte (the first two least significant bits) are reserved for future use and should be set to 0. For Cisco IOS XE Release 2.1, the

Tunnel ToS feature does not conform to this standard and allows you touse the whole ToS byte value, including bits 6 and 7, and to decide to which RFC standard the ToS byte of your packets should conform.

Generic Routing Encapsulation

GRE is defined in RFC 2784. GRE is a carrier protocol that can be used with many different underlying transport protocols and can carry many passenger protocols. RFC 2784 also covers the use of GRE with IPv4 as the transport protocol and the passenger protocol. Cisco software supports GRE as the carrier protocol with many combinations of passenger and transport protocols.

GRE tunnels are described in the following sections:

GRE Tunnel IP Source and Destination VRF Membership

GRE IPv4 Tunnel Support for IPv6 Traffic

GRE Tunnel IP Source and Destination VRF Membership

The GRE Tunnel IP Source and Destination VRF Membership feature allows you to configure the source and destination of a tunnel to belong to any VPN routing and forwarding (VRFs) tables. A VRF table stores routing data for each VPN. The VRF table defines the VPN membership of a customer site that is attached to the network access server (NAS). Each VRF table comprises an IP routing table, a derived Cisco Express Forwarding table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

Prior to Cisco IOS XE Release 2.2, GRE IP tunnels required the IP tunnel destination to be in the global routing table. The implementation of this feature allows you to configure a tunnel source and destination to belong to any VRF. As with existing GRE tunnels, the tunnel becomes disabled if no route to the tunnel destination is defined.

GRE IPv4 Tunnel Support for IPv6 Traffic

IPv6 traffic can be carried over IPv4 GRE tunnels by using the standard GRE tunneling technique to provide the services necessary to implement a standard point-to-point encapsulation scheme. GRE tunnels are links between two points, with a separate tunnel for each point. GRE tunnels are not tied to a specific passenger or transport protocol, but in case of IPv6 traffic, IPv6 is the passenger protocol, GRE is the carrier protocol, and IPv4 is the transport protocol.

The primary use of GRE tunnels is to provide a stable connection and secure communication between two edge devices or between an edge device and an end system. The edge device and the end system must have a dual-stack implementation.

GRE has a protocol field that identifies the passenger protocol. GRE tunnels allow intermediate system to intermediate system (IS-IS) or IPv6 to be specified as the passenger protocol, therebyallowing both IS-IS and IPv6 traffic to run over the same tunnel. If GRE does not have a protocol field, it becomes impossible to distinguish whether the tunnel is carrying IS-IS or IPv6 packets.

EoMPLS over GRE

Ethernet over MPLS (EoMPLS) is a tunneling mechanism that

allows you to tunnel Layer 2 traffic through a Layer 3 MPLS network. EoMPLS is also known as Layer 2 tunneling.
EoMPLS effectively facilitates Layer 2 extension over long distances. EoMPLS over GRE helps you to create the GRE tunnel as hardware-based switched, and encapsulates EoMPLS frames within the GRE tunnel. The GRE connection is established between the two core routers, and then the MPLS label switched path (LSP) is tunneled over.
GRE encapsulation is used to define a packet that has header information added to it prior to being forwarded.
De-encapsulation is the process of removing the additional header information when the packet reaches the destination tunnel endpoint.
When a packet is forwarded through a GRE tunnel, two new headers are added to the front of the packet and hence the context of the new payload changes. After encapsulation, what was originally the data payload and separate IP header are now known as the GRE payload. A GRE header is added to the packet to provide information on the protocol type and the recalculated checksum. A new IP header is also added to the front of the GRE header. This IP header contains the destination IP address of the tunnel.
The GRE header is added to packets such as IP, Layer 2 VPN, and Layer 3 VPN before the header enters into the tunnel. All routers along the path that receives the encapsulated packet use the new IP header to determine how the packet can reach the tunnel endpoint.
In IP forwarding, on reaching the tunnel destination endpoint, the new IP header and the GRE header are removed from the packet and the original IP header is used to forward the packet to the final destination.
The EoMPLS over GRE feature removes the new IP header and GRE header from the packet at the tunnel destination, and the MPLS label is used to forward the packet to the appropriate Layer 2 attachment circuit or Layer 3 VRF.
The scenarios in the following sections describe the L2VPN and L3VPN over GRE deployment on provider edge (PE) or provider (P) routers:
Provider Edge to Provider Edge Generic Routing EncapsulationTunnels
Provider to Provider Generic Routing Encapsulation Tunnels
Provider Edge to Provider Generic Routing Encapsulation Tunnels
Features Specific to Generic Routing Encapsulation
Features Specific to Ethernet over MPLS
Features Specific to Multiprotocol Label Switching Virtual Private Network Provider Edge to Provider Edge Generic Routing EncapsulationTunnels
In the Provider Edge to Provider Edge (PE) GRE tunnels scenario, a customer does not transition any part of the core to MPLS but prefers to offer EoMPLS and basic MPLS VPN services. Therefore, GRE tunneling of MPLS traffic is done between PEs.
Provider to Provider Generic Routing Encapsulation Tunnels

In the Provider to Provider (P) GRE tunnels scenario, Multiprotocol Label Switching (MPLS) is enabled between Provider Edge (PE) and P routers but the network core can either have non-MPLS aware routers or IP encryption boxes. In this scenario, GRE tunneling of the MPLS labeled packets is done between P routers.
Provider Edge to Provider Generic Routing Encapsulation Tunnels in a Provider Edge to Provider GRE tunnels scenario, a network has MPLS-aware P to P nodes. GRE tunneling is done between a PE to P non-MPLS network segment. Features Specific to Generic Routing Encapsulation You should understand the following configurations and information for a deployment scenario:
Tunnel endpoints can be loopbacks or physical interfaces.
Configurable tunnel keepalive timer parameters per endpoint and a syslog message must be generated when the keepalive timer expires.
Bidirectional forwarding detection (BFD) is supported for tunnel failures and for the Interior Gateway Protocol (IGP) that use tunnels.
IGP load sharing across a GRE tunnel is supported.
IGP redundancy across a GRE tunnel is supported.
Fragmentation across a GRE tunnel is supported.
Ability to pass jumbo frames is supported.
All IGP control plane traffic is supported.
IP ToS preservation across tunnels is supported.
A tunnel should be independent of the endpoint physical interface type; for example, ATM, Gigabit, Packet over SONET (POS), and TenGigabit.
Up to 100 GRE tunnels are supported.
Features Specific to Ethernet over MPLS
Any Transport over MPLS (AToM) sequencing.
IGP load sharing and redundancy.
Port mode Ethernet over MPLS (EoMPLS).
Pseudowire redundancy.
Support for up to to 200 EoMPLS virtual circuits (VCs).
Tunnel selection and the ability to map a specific pseudowire to a GRE tunnel.
VLAN mode EoMPLS.
Features Specific to Multiprotocol Label Switching Virtual Private Network Support for the PE role with IPv4 VRF.
Support for all PE to customer edge (CE) protocols.
Load sharing through multiple tunnels and also equal cost IGP paths with a single tunnel.
Support for redundancy through unequal cost IGP paths with a single tunnel.
Support for the IP precedence value being copied onto the expression (EXP) bits field of the Multiprotocol Label Switching (MPLS) label and then onto the precedence bits on the outer IPv4 ToS field of the generic routing encapsulation (GRE) packet.
See the section, "Example: Configuring EoMPLS over GRE" for a sample configuration sequence of EoMPLS over GRE. For more details on EoMPLS over GRE, see the Deploying and Configuring

MPLS Virtual Private Networks
In IP Tunnel Environments document.
Overlay Tunnels for IPv6
The figure below illustrates how overlay tunneling encapsulates IPv6 packets in IPv4 packets for delivery across an IPv4 infrastructure (a core network or the Internet). By using overlay tunnels, you can communicate with isolated IPv6 networks without upgrading the IPv4 infrastructure between them. Overlay tunnels can be configured between border routers or between a border router and a host; however, both tunnel endpoints must support, IPv4 and IPv6 protocol stacks. IPv6 supports the following types of overlay tunneling mechanisms:
6to4
GRE
Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)
IPv4-compatible
Manual
Figure 3
Overlay Tunnels
Note
If the basic IPv4 packet header does not have optional fields, overlay tunnels can reduce the maximum transmission unit (MTU) of an interface by 20 octets. A network that uses overlay tunnels is difficult to troubleshoot. Therefore, overlay tunnels that connect isolated IPv6 networks should not be considered as the final IPv6 network architecture. The use of overlay tunnels is considered as a transition technique for a network that supports either both IPv4 and IPv6 protocol stacks or just the IPv6 protocol stack.
Consult the table below to determine which type of tunnel you want to configure to carry IPv6 packets over an IPv4 network.
Table 1
Suggested Usage of Tunnel Types to Carry IPv6 Packets over an IPv4 Network Tunneling Type
Suggested Usage
Usage Notes
6to4
Point-to-multipoint tunnels that can be used to connect isolated IPv6 sites.
Sites use addresses that begin with the 2002::/16 prefix.
GRE/IPv4
Simple point-to-point tunnels that can be used within a site or between sites.
Tunnels can carry IPv6, Connectionless Network ServiceCLNS, and many other types of packets.
ISATAP
Point-to-multipoint tunnels that can be used to connect systems within a site.
Sites can use any IPv6 unicast addresses.
Manual
Simple point-to-point tunnels that can be used within a site or between sites.
Tunnels can carry IPv6 packets only.

Individual tunnel types are discussed in detail in the following concepts, and we recommend that you review and understand the information on the specific tunnel type that you want to implement. Consult the table below for a summary of the tunnel configuration parameters that you may find useful.

Table 2
Overlay Tunnel Configuration Parameters by Tunneling Type

Overlay Tunneling Type	Overlay Tunnel Configuration Parameter			
	Tunnel Mode	Tunnel Source	Tunnel Destination	Interface Prefix/Address
6to4	ipv6ip 6to4	An IPv4 address or a reference to an interface on which IPv4 is configured.	Not required. These are all point-to-multipoint tunneling types. The IPv4 destination address is calculated, on a per-packet basis, from the IPv6 destination.	An IPv6 address. The prefix must embed the tunnel source IPv4 address.
GRE/IPv4	gre ip	An IPv4 address.	An IPv6 address.	
ISATAP	ipv6ip isatap	Not required. These are all point-to-multipoint tunneling types. The IPv4 destination address is calculated on a per-packet basis from the IPv6 destination.	An IPv6 prefix in modified eui-64 format. The IPv6 address is generated from the prefix and the tunnel source IPv4 address.	
Manual	ipv6ip	An IPv4 address.	An IPv6 address.	

IPv6 Manually Configured Tunnels

A manually configured tunnel is equivalent to a permanent link between two IPv6 domains over an IPv4 backbone. The primary use of a manually configured tunnel is to stabilize connections that require secure communication between two edge routers, or between an end system and an edge router. The manual configuration tunnel also stabilizes connection between remote IPv6 networks.

An IPv6 address is manually configured on a tunnel interface. Manually configured IPv4 addresses are assigned to the tunnel source and destination. The host or router at each end of a configured tunnel must support both the IPv4 and IPv6 protocol stacks. Manually configured tunnels can be configured between border routers or between a border router and a host. Cisco Express Forwarding switching can be used for manually configured IPv6 tunnels. Switching can be disabled if process

switching is required.

Automatic 6to4 Tunnels

An automatic 6to4 tunnel allows isolated IPv6 domains to be connected over an IPv4 network to remote IPv6 networks. The key difference between automatic 6to4 tunnels and manuallyconfigured tunnels is that the tunnel is not point-to-point; it is point-to-multipoint. In automatic 6to4 tunnels, routers are not configured in pairs because they treat the IPv4 infrastructure as a virtual nonbroadcast multiaccess (NBMA) links. The IPv4 address embedded in the IPv6 address is used to find the other end of the automatic tunnel.

An automatic 6to4 tunnel may be configured on a border router in an isolated IPv6 network, which creates a tunnel on a per-packet basis on a border router in another IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the IPv4 address of the border router extracted from the IPv6 address that starts with the prefix 2002::/16, where the format is 2002:border-router-IPv4-address ::/48.The embedded IPv4 addresses are 16 bits and can be used to number networks within the site. The border router at each end of a 6to4 tunnel must support both IPv4 and IPv6 protocol stacks. 6to4 tunnels are configured between border routers or between a border router and a host.

The simplest deployment scenario for 6to4 tunnels is to interconnect multiple IPv6 sites, each of which has at least one connection to a shared IPv4 network. This IPv4 network could either be the Internet or a corporate backbone. The key requirement is that each site have a globally unique IPv4 address; the Cisco software uses this address to construct a globally unique 6to4/48 IPv6 prefix. A tunnel with appropriate entries in a Domain Name System (DNS) that maps hostnames and IP addresses for both IPv4 and IPv6 domains, allows the applications to choose the required address IPv6 traffic can be carried over IPv4 GRE tunnels by using the standard GRE tunneling technique to provide the services necessary to implement a standard point-to-point encapsulation scheme. GRE tunnels are links between two points, with a separate tunnel for each point. GRE tunnels are not tied to a specific passenger or transport protocol, but in case of IPv6 traffic, IPv6 is the passenger protocol, GRE is the carrier protocol, and IPv4 is the transport protocol.

The primary use of GRE tunnels is to provide a stable connection and secure communication between two edge devices or between an edge device and an end system. The edge device and the end system must have a dual-stack implementation. GRE has a protocol field that identifies the passenger protocol. GRE tunnels allow intermediate system to intermediate system (IS-IS) or IPv6 to be specified as the passenger protocol, thereby allowing both IS-IS and IPv6 traffic to run over the same tunnel. If GRE does not have a protocol field, it becomes impossible to distinguish whether the tunnel is carrying IS-IS or IPv6 packets.

NEW QUESTION: 3
A project team is developing requirements of the new version of a web application used by internal and external users. The application already features username and password requirements for login, but the organization is required to implement multifactor authentication to meet regulatory requirements. Which of the following would be added requirements will satisfy the regulatory requirement? (Choose three.)
A. Tokenized mobile device
B. Digital certificate
C. Rule-based access control
D. Keystroke dynamics
E. Identity verification questions
F. Increased password complexity
G. Personalized URL
H. Time-of-day restrictions
Answer: A,B,E

NEW QUESTION: 4
The administrator cannot use telnet to manage the AR2200. The administrator is able to verify connectivity to the router and has been informed that other administrators have no difficulties using telnet. Which statements describe the possible reasons for this problem? (Multiple Choice)
A. The user's status has been blocked.
B. The user has been deleted.
C. The user's priviledge level has been changed to 0.
D. The telnet service in the AR2200 router has been disabled.
Answer: A,B

C-TS462-1909 Reliable Exam Simulator
Valid 156-915.80 Study Plan
Valid 1Z0-1079-20 Study Guide
C-ARP2P-2108 Questions
DES-1241 High Quality