

Cisco 642-504

**642-504 Securing Networks with Cisco Routers and
Switches**

Practice Test

Version 2.5

QUESTION NO: 1

Which two technologies can secure the control plane of the Cisco router? (Choose two. r

- A. BPDU protection
- B. role-based access control
- C. routing protocol authentication
- D. CPPr

Answer: C,D

QUESTION NO: 2

Cisco Secure Access Control Server (ACS) is a highly scalable, high-performance access control server that provides a comprehensive identity networking solution. Which of these statements is correct regarding user setup on ACS 4.0?

- A. Users are assigned to the default group.
- B. A user can belong to more than one group.
- C. The username can contain characters such as "#" and "?".
- D. The settings at the group level override the settings configured at the user level

Answer: A

QUESTION NO: 3

Please study the exhibit carefully, and then answer the following question: .

The screenshot shows the 'About Your Router' page in Cisco Configuration Manager. The host name is 'Isr2811'. The page is divided into 'Hardware' and 'Software' sections. Hardware details include Model Type (Cisco 2811), Available/Total Memory (87/256 MB), and Total Flash Capacity (61 MB). Software details include IOS Version (12.4(15)T5) and SDM Version (2.4). A 'Feature Availability' bar at the bottom shows icons for IP, Firewall, VPN, IPS, and NAC, all of which are active.

Hardware	More...	Software	More...
Model Type:	Cisco 2811	IOS Version:	12.4(15)T5
Available / Total Memory(MB):	87/256 MB	SDM Version:	2.4
Total Flash Capacity:	61 MB		

Feature Availability: IP [Active] Firewall [Active] VPN [Active] IPS [Active] NAC [Active]

The screenshot shows the 'VPN' configuration page in Cisco Configuration Manager. The left sidebar contains a tree view of VPN-related tasks, including Site-to-Site VPN, Easy VPN Remote, Easy VPN Server, Dynamic Multipoint VPN, SSL VPN, and VPN Components. The main content area is titled 'Virtual Private Network' and provides a definition of VPN and a list of supported technologies: IPsec (site-to-site) VPN, GRE over IPsec, Dynamic Multipoint VPN, Easy VPN, and Cisco SSL VPN. A 'VPN Design Guide' section at the bottom features a 'Launch Design Guide' button.

Virtual Private Network

A Virtual Private Network (VPN) creates a secure connection over an insecure public network, such as the Internet. Traffic sent through a VPN is encrypted and it cannot be read by anyone who is not on the VPN.

VPN technologies include:

- *IPsec (site-to-site) VPN
- *GRE over IPsec
- *Dynamic Multipoint VPN
- *Easy VPN
- *Cisco SSL VPN

The VPN Design Guide can help you to decide which type of VPN to set up.

VPN Design Guide:

Click [Launch Design Guide] to begin.

[Launch Design Guide](#)

The screenshot shows the 'Protocol Inspection Policy Maps' configuration window. The left pane shows a tree view with 'Protocol Inspection' selected. The main pane shows a table of Policy Map Names and a details section for the 'testpm' policy map.

Policy Map Name	Description
testpm	

Details of Policy Map: testpm

Match Class Name	Action
httpclass	inspect
etherclass	inspect
icmpclass	Pass
class-default	Drop

www.pass4sures.com

Refer to the appropriate SDM screen(s), which two statements correctly describe the Cisco IOS Zone-Based Firewall configuration? (Choose two)

- A. The "reset" action is applied to any HTTP request sourced from the "in" zone and destined to the "out" zone, which also has a request Uniform Resource Identifier (URI) that is greater than 500 bytes in length.
- B. The "inspect" action is applied to Internet Control Message Protocol (ICMP) traffic sourced from the "in" zone and destined to the "out" zone.
- C. The "http-policy" inspection policy map is applied to all HTTP and HTTPS traffic sourced from the "in" zone and destined to the "out" zone.
- D. The "testpm" inspection policy map is applied to the 'in/out' zone-pair.

Answer: A,D

QUESTION NO: 4

Refer to the appropriate SDM screen(s), what is the User Datagram Protocol (UDP) idle time set for any HTTP traffic that is sourced from the "in" zone and destined to the "out" zone?

About Your Router
Host Name: isr2011



Cisco 2811

	Hardware	Model	Software	Model
Model Type:	Cisco 2811		IOS Version:	12.4(15)T5
Available / Total Memory(MB):	87/256 MB		SDM Version:	2.4
Total Flash Capacity:	61 MB			

Feature Availability:
IPsec ✔
Firewall ✔
VPN ✔
IPS ✔
NAC ✔

Configuration Overview
View Running Config

Interfaces and Connections
Up (2) Down (1)

Total Supported LAN:	1	Total Supported WAN:	1 (10/100Ethernet0)
Configured LAN Interface:	1	Total WAN Connections:	1
DHCP Server:	Configured		

Firewall Policies
Active

VPN
Up (0)

IPSec (Site-to-Site):	0	GRE over IPSec:	0
Auth Login Required:	0	Easy VPN Remote:	0
No. of DMVPN Clients:	0	No. of Active VPN Clients:	0

Routing

No. of Static Route:	0		
Dynamic Routing Protocols:	None		

Intrusion Prevention

Total Active Signatures:	332		
No. of IPS-enabled Interfaces:			
Signature Version:	9310.0		

- VPN
- Site-to-Site VPN
- Easy VPN Remote
- Easy VPN Server
- Dynamic Multipoint VPN
- SSL VPN
- SSL VPN Gateways
- Packages
- VPN Components
- IPSec
- IPSec Policies (Crypto)
- Dynamic Crypto Maps
- IPSec Profiles
- Transform Sets
- IPSec Rules (ACLs)
- IKE
- IKE Policies
- Pre-shared Keys
- IKE Profiles
- Easy VPN Server
- Group Policies
- Browser Proxy Settings
- Public Key Infrastructure
- Certificate Authority
- Certificate Enrollment
- Router Certificates
- RSA Keys
- USB Tokens
- VPN Keys Encryption

Virtual Private Network

A Virtual Private Network (VPN) creates a secure connection over an insecure, public network, such as the Internet. Traffic sent through a VPN is encrypted and it cannot be read by anyone who is not on the VPN.

VPN technologies include:

- *IPsec (site-to-site) VPN
- *GRE over IPsec
- *Dynamic Multipoint VPN
- *EasyVPN
- *Cisco SSL VPN

The VPN Design Guide can help you to decide which type of VPN to set up.



Click Launch Design Guide to begin.

[Launch Design Guide...](#)

Parameter Map

Inspect Settings Parameter Maps Add Edit Delete

Parameter Map Name	Used By
inspect	HTTP

Details of Parameter Map: inspect

Item Name	Item Value
Alert	On
AlertTime	30
TCP Synwait Timeout	30
TCP Finwait Timeout	30
TCP Idle Timeout	3600
UDP Idle Timeout	30
DNS Timeout	30
ICMP Idle Timeout	5

HTTP Protocol Application Service Groups Add Edit Delete

Class Map Name	Used By
inspect	HTTP

Details of Class Map: inspect

Item Name	Item Value
Request	
Req-Method	Disabled
URI	Length > 500
Response	
Req-Flags	
Ports/NoPorts	Disabled

www.pass4sures.com

Protocol Inspection Policy Maps Add Edit Delete

Policy Map Name	Description
inspect	

Details of Policy Map: inspect

Match Class Name	Action
inspectclass	Inspect
otherclass	Inspect
inspectclass	Pass
class-default	Drop

www.pass4sures.com

- A. 10 seconds
- B. 15 seconds
- C. 30 seconds

D. 35 seconds

Answer: D

QUESTION NO: 5

Refer to the appropriate SDM screen(s), what is the reason that outside hosts can't initiate Telnet (port 23) traffic to the 172.16.1.10 inside host?

About Your Router Host Name: isr2811

Hardware	More...	Software	More...
Model Type:	Cisco 2811	IOS Version:	12.4(15)T5
Available / Total Memory(MB):	87/256 MB	SDM Version:	2.4
Total Flash Capacity:	61 MB		

Feature Availability: IP [On] Firewall [On] VPN [On] IPS [On] NAC [On]

Configuration Overview View Running Config

Category	Status	Count	Details
Interfaces and Connections	Up (2) / Down (1)		
Total Supported LAN:		1	
Configured LAN Interface:		1	
DHCP Server:		Configured	
Total Supported WAN:		1 (10/100Ethernet)	
Total WAN Connections:		1	
Firewall Policies	Active		
VPN	Up (0)		
IPSec (Site-to-Site):		0	
GRE over IPSec:		0	
Auth Login Required:		0	
Easy VPN Remote:		0	
No. of DMVPN Clients:		0	
No. of Active VPN Clients:		0	
Routing			
No. of Static Routes:		0	
Dynamic Routing Protocols:		None	
Intrusion Prevention			
Total Active Signatures:		332	
No. of IPS-enabled Interfaces:		3	
Signature Version:		6.3(1)0	

VPN

- VPN
 - Site-to-Site VPN
 - Easy VPN Remote
 - Easy VPN Server
 - Dynamic Multipoint VPN
 - SSL VPN
 - SSL VPN Gateways
 - Package
 - VPN Components
 - IPSec
 - IPSec Policies (Crypto)
 - Dynamic Crypto Ma
 - IPSec Profiles
 - Transform Sets
 - IPSec Rules (ACL)
 - IKE
 - IKE Policies
 - Pre-shared Keys
 - IKE Profiles
 - Easy VPN Server
 - Group Policies
 - Browser Proxy Set
 - Public Key Infrastructu
 - Certificate Authority
 - Certificate Enrollme
 - Router Certificates
 - RSA Keys
 - USB Tokens
 - VPN Keys Encryption

Virtual Private Network

A Virtual Private Network (VPN) creates a secure connection over an insecure, public network, such as the Internet. Traffic sent through a VPN is encrypted and it cannot be read by anyone who is not on the VPN.

VPN technologies include:

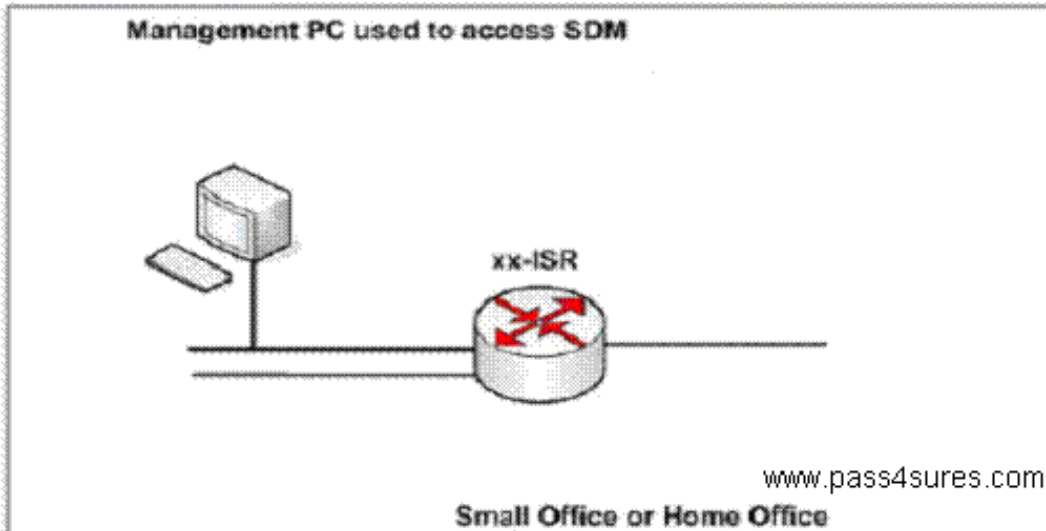
- *IPSec (site-to-site) VPN
- *GRE over IPsec
- *Dynamic Multipoint VPN
- *Easy VPN
- *Cisco SSL VPN

The VPN Design Guide can help you to decide which type of VPN to set up.

VPN Design Guide

Click Launch Design Guide to begin.

[Launch Design Guide...](#)



V

Results of "show running-config"

```

ip http secure-server
ip http timeout-policy idle 60 life 86400 requests 10000
ip nat inside source list 1 interface FastEthernet0/1 overload
ip nat inside source static tcp 172.16.1.10 23 interface FastEthernet0/1 23

access-list 1 permit 172.16.1.0 0.0.0.255
access-list 23 permit host 172.16.1.11
access-list 23 permit host 172.16.1.13
    
```

control-plane

- Router Properties
- Router Access
- Secure Device Provisioning
- OSPF
- OSPF
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mapping
- Router Redundancy
- SD-WAN
- AAA
- Local Pools
- Router Redundancy
- SD-WAN
- CSPL
- Policy Map
- Class Map
- Platform Tools**
 - Inspect
 - Process ID
 - URL Filtering
 - Regular Expressions
- Configuration Management

Forwarder Map

Inspect Settings Forwarder Map

Parameter Map Name	Used By
172.16.1	172.16.1

Default v1 Parameters Map Settings

Item Name	Item Value
Alert	On
Accounting	100
TCP Deny wait timeout	30
TCP Forward timeout	10
TCP idle timeout	3000
TCP idle timeout	30
DNS timeout	10
ICMP idle timeout	5

www.pass4sures.com