

Cisco 640-553

**640-553 IINS Implementing Cisco IOS Network
Security**

Practice Test

Version 14.25

QUESTION NO: 1

Which access list will permit HTTP traffic sourced from host 10.1.129.100 port 3030 destined to host 192.168.1.10?

- A. access-list 101 permit tcp any eq 3030
- B. access-list 101 permit tcp 10.1.128.0 0.0.1.255 eq 3030 192.168.1.0 0.0.0.15 eq www
- C. access-list 101 permit tcp 10.1.129.0 0.0.0.255 eq www 192.168.1.10 0.0.0.0 eq www
- D. access-list 101 permit tcp host 192.168.1.10 eq 80 10.1.0.0 0.0.255.255 eq 3030
- E. access-list 101 permit tcp 192.168.1.10 0.0.0.0 eq 80 10.1.0.0 0.0.255.255
- F. access-list 101 permit ip host 10.1.129.100 eq 3030 host 192.168.1.100 eq 80

Answer: B

QUESTION NO: 2 DRAG DROP

Drag three proper statements about the IPsec protocol on the above to the list on the below.

IPsec is a framework of open standards.

IPsec is bound to specific encryption algorithms, such as 3DES and AES.

IPsec ensures data integrity by using checksums.

IPsec authenticates users and devices that can carry out communication independently.

IPsec is implemented at Layer 4 of the OSI model.

IPsec uses digital certificates to guarantee confidentiality.

Drag and drop question. Drag the items to the proper locations.

www.pass4sures.com

Answer:

IPsec is a framework of open standards.

IPsec is bound to specific encryption algorithms, such as 3DES and AES.

IPsec ensures data integrity by using checksums.

IPsec authenticates users and devices that can carry out communication independently.

IPsec is implemented at Layer 4 of the OSI model.

IPsec uses digital certificates to guarantee confidentiality.

Drag and drop question. Drag the items to the proper locations.

IPsec is a framework of open standards.

IPsec ensures data integrity by using checksums.

IPsec authenticates users and devices that can carry out communication independently. www.pass4sures.com

QUESTION NO: 3

In a brute-force attack, what percentage of the keyspace must an attacker generally search through until he or she finds the key that decrypts the data?

- A. Roughly 50 percent
- B. Roughly 66 percent
- C. Roughly 75 percent
- D. Roughly 10 percent

Answer: A


QUESTION NO: 4

The information of Cisco Router and Security Device Manager(SDM) is shown below:

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

About Your Router Host Name: R1



Cisco 2811

Hardware	More...	Software	More...
Model Type:	Cisco 2811	IOS Version:	12.4(24)T3
Available / Total Memory(MB):	71/256 MB	SDM Version:	2.5
Total Flash Capacity:	61 MB		

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

Configuration Overview View Running Config

Interfaces and Connections ✔ Up (3) ✘ Down (10)

Total Supported LAN: 2 **Total Supported WAN:** 6
Configured LAN Interface: 2 **Total WAN Connections:** 0
DHCP Server: Not Configured

Firewall Policies ✔ Active

Zone Pair's	Source Zone	Destination Zone	Policy Name
sdm-zp-gre-out	gre-zone	out-zone	sdm-permit-gre
sdm-zp-out-self	out-zone	self	sdm-permit
sdm-zp-in-out	in-zone	out-zone	sdm-inspect

VPN ✔ Up (0)

IPSec (Site-to-Site): 0 **GRE over IPSec:** 1
Xauth Login Required: 0 **Easy VPN Remote:** 0
No. of DMVPN Clients: 0 **No. of Active VPN Clients:** 0


Routing **Intrusion Prevention**

No. of Static Route: 2 **Total Active Signatures:** 558
Dynamic Routing Protocols: EIGRP **No. of IPS-enabled Interfaces:** 2
Signature Version: 5414.0

www.pass4sures.com

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help



Tasks **Additional Tasks**

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones**
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Configuration Management

Zone Add... Edit... Delete

Name	Associated Interfaces	Associated Zone Pairs
Inbound		
gre-zone		sdm-zp-out-gre, sdm-zp-in-gre1, sdm-zp-gre-out, sdm-
Outbound		
out-zone	FastEthernet0/1	sdm-zp-self-out, sdm-zp-out-gre, sdm-zp-VPNOutside
in-zone	FastEthernet0/0	sdm-zp-in-gre1, sdm-zp-VPNOutsideToInside-1, sdm-

www.pass4sures.com

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks

- Interfaces and Connections
- Firewall and RCL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

Additional Tasks

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
 - QoS Policy Map
 - Protocol Inspection
 - Application Inspection
 - HTTP
 - IM
 - P2P
 - SMTP
 - RPC
 - IMAP
 - POP3
 - Class Map
 - QoS Class Map
 - Inspection
 - Deep Packet Inspection
 - HTTP
 - IM
 - P2P
 - SMTP
 - RPC
 - IMAP
 - POP3
 - Parameter Map
- Configuration Management

Inspect Class Maps Add... Edit... Delete

Class Map Name	Used By
sdm-protocol-p2p	sdm-inspect
SDM_SSH	
SDM_VPN_TRAFFIC	
sdm-cls-icmp-access	
SDM_IP	sdm-permit-ip
SDM_GRE	sdm-permit-gre
SDM_ESP	
SDM-Voice-permit	sdm-inspect
sdm-cls-protocol-p2p	

Details of Class Map: sdm-cls-icmp-access

Item Name	Item Value
Match Protocol	icmp
Match Protocol	tcp
Match Protocol	udp
Match Protocol	https
Match Protocol	smtp
Match Protocol	pop3
Match Protocol	dns
Match Protocol	sql-net
Match Protocol	ftp
Match Protocol	shell
Match Protocol	h323
Match Protocol	cuseeme
Match Protocol	http
Match Protocol	imap
Match Protocol	ntp
Match Protocol	bootpc
Match Protocol	ms-sql
Match Protocol	ms-sql-m
Match Protocol	netbios-ssn
Match Protocol	netbios-dgm

Configuration delivered to router. www.pass4sures.com
13:57:07 UTC Fri Aug 20 2010

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks

- Interfaces and Connections
- Firewall and RCL
- VPN
- Security Audit
- Routing
- NAT
- Intrusion Prevention
- Quality of Service
- NAC
- Additional Tasks

Additional Tasks

- Router Properties
- Router Access
- Secure Device Provisioning
- DHCP
- DNS
- Dynamic DNS Methods
- ACL Editor
- Port to Application Mappings
- Zone Pairs
- Zones
- AAA
- Local Pools
- Router Provisioning
- 802.1x
- C3PL
- Policy Map
 - QoS Policy Map
 - Protocol Inspection
 - Application Inspection
 - HTTP
 - IM
 - P2P
 - SMTP
 - RPC
 - IMAP
 - POP3
 - Class Map
 - QoS Class Map
 - Inspection
 - Deep Packet Inspection
 - HTTP
 - IM
 - P2P
 - SMTP
 - RPC
 - IMAP
 - POP3
 - Parameter Map
- Configuration Management

Protocol Inspection Policy Maps Add... Edit... Delete

Policy Map Name	Description
sdm-permit-dmzservice	
sdm-permit-icmpreply	
sdm-permit	
sdm-inspect	

Details of Policy Map: sdm-permit

Match Class Name	Action
SDM_CA_SERVER	Pass
class-default	Drop

www.pass4sures.com

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks **Additional Tasks**

- Router Properties
 - Router Access
 - Secure Device Provisioning
 - DHCP
 - DNS
 - Dynamic DNS Methods
 - ACL Editor
 - Port to Application Mappings
 - Zone Pairs
 - Zones
 - AAA
 - Local Pools
 - Router Provisioning
 - 802.1x
 - C3PL
 - Policy Map
 - QoS Policy Map
 - Protocol Inspection**
 - Application Inspection
 - Class Map
 - QoS Class Map
 - Inspection
 - Deep Packet Inspection
 - Parameter Map
 - Configuration Management

Protocol Inspection Policy Maps Add... Edit... Delete

Policy Map Name	Description
sdm-permit-dmzservice	
sdm-permit-icmpreply	
sdm-permit	
sdm-inspect	

Details of Policy Map: sdm-permit

Match Class Name	Action
SDM_CA_SERVER	Pass
class-default	Drop

www.pass4sures.com

File Edit View Tools Help

Home Configure Monitor Refresh Save Search Help

Tasks **Additional Tasks**

- Router Properties
 - Router Access
 - Secure Device Provisioning
 - DHCP
 - DNS
 - Dynamic DNS Methods
 - ACL Editor
 - Port to Application Mappings
 - Zone Pairs
 - Zones
 - AAA
 - Local Pools
 - Router Provisioning
 - 802.1x
 - C3PL
 - Policy Map
 - QoS Policy Map
 - Protocol Inspection
 - Application Inspection
 - Class Map
 - QoS Class Map
 - Inspection**
 - Deep Packet Inspection
 - Parameter Map
 - Configuration Management

Inspect Class Maps Add... Edit... Delete

Class Map Name	Used By
sdm-clis-insp-traffic	
sdm-protocol-http	sdm-inspect
sdm-icmp-access	sdm-permit-icmpreply
SDM_CA_SERVER	sdm-permit
sdm-invalid-src	sdm-inspect
sdm-insp-traffic	sdm-inspect
sdm-dmz-traffic	sdm-permit-dmzservice
sdm-protocol-pop3	sdm-inspect

Details of Class Map: sdm-invalid-src

Item Name	Item Value
Match ACL	100

www.pass4sures.com

ID	Source	Destination	Service	Action	Rule Options	
sdm-permit-icmpreply (self to out-zone)						
1	any	any	icmp tcp udp	Permit Firewall		
2	Unmatched Traffic					Permit ACL
sdm-permit-dmzservice (out-zone to dmz-zone, in-zone to dmz-zone)						
1	any	192.168.1.100	http	Permit Firewall		
2	Unmatched Traffic					Drop
sdm-permit (out-zone to self)						
1	class-Map: SDM_CA_SERVER			Permit ACL		
2	Unmatched Traffic					Drop
sdm-inspect (in-zone to out-zone)						
1	<ul style="list-style-type: none"> 255.255.255.255 -> any 127.0.0.0/0.255.255.255 -> any 10.1.2.0/0.0.0.255 -> any 192.168.1.0/0.0.0.255 -> any 			any	Drop	Log
2	any	any	http	Permit Firewall		
3	any	any	smtp	HTTP Application I...		
4	any	any	imap	SMTP Application I...		
5	any	any	pop3	Permit Firewall		
6	any	any	sdm-cl-protocol-p2p	IMAP Application I...		
				POP3 Application I...		
				Drop	Log	

Policy Map Name	Description
sdm-permit-dmzservice	
sdm-permit-icmpreply	
sdm-permit	
sdm-inspect	

Match Class Name	Action
sdm-invalid-src	Drop/Log
sdm-protocol-http	Inspect
sdm-protocol-smtp	Inspect
sdm-protocol-imap	Inspect
sdm-protocol-pop3	Inspect
sdm-protocol-p2p	Drop/Log
sdm-protocol-im	Drop/Log
sdm-insp-traffic	Inspect
SDM-Voice-permit	Inspect
class-default	Pass

Within the "sdm-permit" policy map, what is the action assigned to the traffic class "class-default"?

- A. inspect
- B. pass
- C. drop
- D. police
- E. log

Answer: C

QUESTION NO: 5 DRAG DROP

On the basis of the description of SSL-based VPN, place the correct descriptions in the proper locations.

The authentication process uses hashing technologies.

You can also use the application programming interface to extensively modify the SSL client software for use in special applications.

Asymmetric algorithms are used for authentication and key exchange.

SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router.

Symmetric algorithms are used for bulk encryption.

SSL-based VPNs.

www.pass4sures.com

Answer:

The authentication process uses hashing technologies.

You can also use the application programming interface to extensively modify the SSL client software for use in special applications.

Asymmetric algorithms are used for authentication and key exchange.

SSL VPNs and IPsec VPNs cannot be configured concurrently on the same router.

Symmetric algorithms are used for bulk encryption.

SSL-based VPNs.

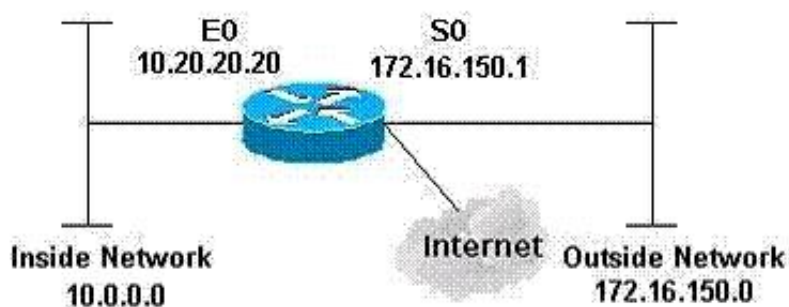
The authentication process uses hashing technologies.

Asymmetric algorithms are used for authentication and key exchange.

Symmetric algorithms are used for bulk encryption.

QUESTION NO: 6

Refer to the exhibit and partial configuration. Which statement is true?



```
interface Ethernet0
ip address 10.20.20.20 255.255.255.0
ip access-group 101 in
...
access-list 101 permit tcp 10.20.20.0 0.0.0.255 any
access-list 101 permit udp 10.20.20.0 0.0.0.255 any
access-list 101 permit icmp 10.20.20.0 0.0.0.255 any
```

- A. All traffic destined for network 172.16.150.0 will be denied due to the implicit deny all.
- B. All traffic from network 10.0.0.0 will be permitted.
- C. Access-list 101 will prevent address spoofing from interface E0.
- D. This is a misconfigured ACL resulting in traffic not being allowed into the router in interface S0.
- E. This ACL will prevent any host on the Internet from spoofing the inside network address as the source address for packets coming into the router from the Internet.

Answer: C

QUESTION NO: 7

Which of these can be used to authenticate the IPsec peers during IKE Phase 1?

- A. Diffie-Hellman Nonce
- B. pre-shared key
- C. XAUTH
- D. integrity check value
- E. ACS
- F. AH

Answer: B

Explanation:

Internet Key Exchange (IKE) executes the following phases:

- + IKE Phase 1: Two IPsec peers perform the initial negotiation of SAs. Phase 1 generates an Internet Security Association and Key Management Protocol (ISAKMP) SA, used for management traffic. Public key techniques or, alternatively, a pre-shared key, are used to mutually authenticate the communicating parties. Phase 1 operates in either Main Mode or Aggressive Mode. Main Mode protects the identity of the peers, Aggressive Mode does not.
- + IKE Phase 2: SAs are negotiated by the IKE process ISAKMP on behalf of other services, such as IPsec, that need encryption key material for operation. IKE Phase 2 is used to build IPsec SAs, which are for passing end-user data. Additional service negotiations occur in IKE Phase 1, DPD, Mode Config, and so on

QUESTION NO: 8

Which description about asymmetric encryption algorithms is correct?

- A. They use the same key for encryption and decryption of data.
- B. They use different keys for decryption but the same key for encryption of data.
- C. They use different keys for encryption and decryption of data.