

Cisco 642-825

CISCO 642-825 ISCW - Implementing Secure Converged Wide Area Networks

Practice Test

Version 2.1

https://certkill.com



QUESTION NO: 1

What technology must be enabled as a prerequisite to running MPLS on a Cisco router?

- A. process switching
- B. CEF switching
- C. fast switching
- D. cache driven switching
- E. routing-table driven switching

Answer: B

Explanation:

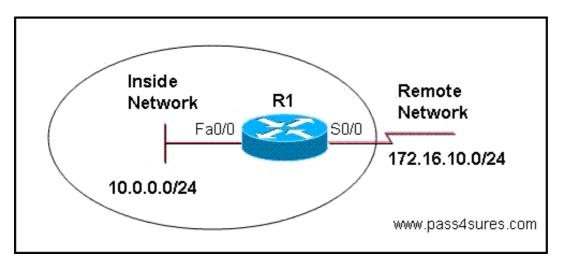
Configuring Cisco Express Forwarding To enable MPLS, you must first enable Cisco Express Forwarding (CEF) switching.

Reference: "CCNP ISCW Portable Command Guide" By Scott Empson, Hans Roth. http://www.ciscopress.com/articles/article.asp?p=1180984

QUESTION NO: 2

Refer to the exhibit.

Which ACL configuration will prevent a DoS TCP SYN attack from a spoofed source into the internal network?



- A. R1(config)# access-list 120 deny icmp any any echo log
- R1(config)# access-list 120 deny icmp any any redirect log
- R1(config)# access-list 120 permit icmp any 10.0.0.0 0.0.255
- R1(config)# interface Serial0/0
- R1(config-if)# ip access-group 120 in
- B. R1(config)# access-list 120 permit tcp any 172.16.10.0 0.0.0.255 established
- R1(config)# access-list 120 deny ip any any log

R1(config)# interface FastEthernet0/0

R1(config-if)# ip access-group 120 in

C. R1(config)# access-list 120 deny ip any host 10.0.0.255 log

R1(config)# access-list 120 permit ip any 10.0.0.0 0.0.255 log

R1(config)# interface Serial0/0

R1(config-if)# ip access-group 120 in

D. R1(config)# access-list 120 deny udp 10.0.0.0 0.0.255.255 host 255.255.255.255 eq 512

R1(config)# interface Serial0/0

R1(config-if)# ip access-group 120 in

Answer: B

Explanation:

The TCP SYN Attack

When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake."

While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.

The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Since the SYN ACK is destined for an incorrect or non-existent host, the last part of the "three-way handshake" is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. By generating phony TCP SYN packets from random IP addresses at a rapid rate, it is possible to fill up the connection queue and deny TCP services (such as e-mail, file transfer, or WWW) to legitimate users.

There is no easy way to trace the originator of the attack because the IP address of the source is forged.

In this example, this type of attack could be stopped since we are allowing only traffic that was originated by the internal (fa0/0) network destined to the R1 branch network with the use of the "established" keyword.

QUESTION NO: 3

This item contains several questions that you must answer. You can view these questions by clicking on the Questions button to the left. Changing questions can be accomplished by clicking the numbers to the left of each question. In order to complete the questions, you will need to refer to the SDM and the topolgy, neither of which is currently visible.

CERTKILL

To gain access to either the topology or the SDM, click on the button to left side of the screen that corresponds to the section you wish to access. When you have finished viewing the topolgy or the SDM, you can return to your questions by clicking on the Questions button to the left.

Instructions	G Cisco Route	r and Security Device Mana ols Help	eger (SDM)				
	💰 Home		itor O Refresh	Save Sea	rch Help		Disco Systems
Questions	Tasks	E Firewall and ACL	(Tentest)	0010 000	iur nop		
	-	Create Firewall Edit Firewall	Policy / ACL Appl	cation Security			
	Interfaces and	Select a direction From:	FastEthernet0/0	• EL TO.	Serial0.0.0	- 64, Go	View Option
Cisco SDM 5.0	Errowell and ACL	Originating traffic	-	FastEthernet0/0	Serie	000	_
Topology	VPN	Returning traffic	IOS F		rom FastEthernet0		
	500	Firewall Feature Availability	The second s	Access Rule:	100	G Inspection Rule	and the second se
	Security Audit	Services	200000000000000000000000000000000000000	ide X Cut RaC		FastEthernet0/0 - inbound	and the second se
	Routing	Action Source	255 255 255 ****	7 7	- 10 - 0	Log Option	Description
	NAT	Permit Aany	*an	Y I	e p		
	Entrusion Prevention	Applications		⊕ Add + (a Edit 📋 Delete	Global Settings	ESummary Details
	-	Application Protocol	Alert	Audit Trail	Timeout	Description	
	Quality of Service	dros frp h223 https				CUSeeMe Protocol Domain Name Serve File Transfer Protocol H.323 Protocol (e.g. HTTPS Protocol	n al MS NetMeeting, Intel V
Cisco Systems	60	1 a			•	a survey backward	
A AL	Additional Tasks			Apply Changes	Discard Change	www.pa	ass4sures.com
	Firewall and ACL					14.28.57 UTC	Mon Nov 13 2006

Home	Configure Monito	r Refresh	Save Sea	arch	? Help		CISCO SYSTEM
Tasks	C Firewall and ACL						
Sec.	Create Firewall Edit Firewall Po	licy / ACL API	plication Security				
Interfaces and	Select a direction From: Fa	stEthernet0/0	- K To	Seria	0.0.016	- Ict Go	View Option
			FastEthernet0/0	,	Serial0	oron	
rewall and ACL	Originating traffic		- 200				-
	Returning traffic	*	i				
VPN	And the Rest of the Local Division of the Rest of the		Firewall : Active (F	the state of the state of the	stEthemet0/0		
100	Firewall Feature Availability:	Available	Access Rule:	101		 Inspection Rul 	e: SDM_LOW
Security Audit	Services	⇔Add • ≣	Edit X Cut Sta	Copy II	B Patter 1	Serial0/0/0 - inbound	·) All Apply Firmul
000	Action Source	De	stination	Service	Lo	g Option	Description
Routind	Deny 10.79 223 0/0 0		any	ip ip		ni 1. 1052100514	
	Permit * any		172.16.81.108	100 et	cho-reply/icmp me-exceede	C	
1.	✓ Permit ★ any ✓ Permit ★ any		172.16.81.108		nreachable		
NAT	Deny \$10,0.000255.3	255.255	t any	🦛 ip	1000000000		
	Deny + 172.16.0.0/0.15	255.255	r any	🚁 ip	l		•
	•1						(•)
	Applications		🗢 Add =	GE Edit	1 Delete	G Global Settings	ESummary Details
	Application Protocol	Alert	Audit Trail	-	Timeout	Description	
	cuseeme					CUSeeMe Protoco	
ality of Service	dns					Domain Name Sen	
340	ftp h323					File Transfer Proto	
	https					H.323 Protocol (e.g HTTPS Protocol), MS NetMeeting, Intel V
	Linear an					IOMD Destand	•
6	•			10			

Cisco 642-825: Practice Exam



Home	Configure	Monitor Refre	esh Save	Search	P Help		Cisco Syste
asks	Firewall and ACL		Cure	Contra		and the second	
Sec.	Create Firewall Edit Fi	rewall Policy / ACL	Application Secu	rity			
ertables and	Select a direction Fr	rom: [FastEthernet	00 · C	To: Seri	o/0/0le	· Go	View Option
9			FastEther	01019	Serial	0/0/0	
elland AC	Onginating of			>			
VPN	Returning traf	KC .	IOS Firewall : Act	1 Comments	- En		
-	Firewall Feature Avail	ability: Available	Access R	the state of the s	SIE THEITHEIGH	 Inspection Rule 	SDM LOW
unity Audit	Services		E Edit X Cut	when whether have	C. Dauba - 1	Serial0/0/0 - inbound	· Jan, Aught Floren
	Action Source		Destination	Service		og Option	Description
000	U Deny - 1/2.10	0.00.15.255.250	w uny	M. 4		og ropoon	Description
Routing		8.0.00.0.255.255 0.00.255.255.255	★ any ★ any				
11	Deny 3255.25	5.255.255	🛪 any	are ig			
NAT	O Denv ≍0.0.0.0 Denv ★any	15	* any * any			CI Log	
			a bity		,	ca coy	
0			1000				
				id - 🖬 Edit	the second se	Global Settings	Summary Detail
- 6	Application Protocol	Alert	Audit	Trail	Timeout	Description	
of Servic	cuseeme dns					CUSeeMe Protocol Domain Name Serv	
and the second second	ftp					File Transfer Protoc	
Sar	h323					H.323 Protocol (e.g.	MS NetMeeting, Intel V
NAC	https					HTTPS Protocol	
1000	•			-10			
60	and the second sec						

Cisco Router and Security Device Manager (SDM) 103 File Edit View Tools Help STEED SYSTEMS Configure Monitor Refresh Save Q Search 🛃 Home Help als. .de Tasks E Firewall and ACL Create Firewall Edit Firewall Policy / ACL Application Security 4 Select a direction From: FastEthemet0/0 To: Serial0.0.0 - 62 Go View Option FastEthernet0/0 Seria10/0/0 Originating traffic - Returning traffic -420 IOS Firewall : Active (From FastEthernet0/0 to Serial0/0/0) Round State Firewall Feature Availability: Available Caress Rule: 101 Q Inspection Rule: SDM_LOW Add - E Edit X Cut Sta Copy 19. Part Services Serial0/0/0 - inbound · 6.10
 Action
 Source
 Destination

 Deny
 + 172.10.0.00.15.253.256
 # any

 Deny
 + 192.168.0.00.0.255.255
 # any

 Deny
 + 192.168.0.00.0.255.255
 # any

 Deny
 + 127.0.0.00.255.255
 # any

 Deny
 + 127.0.0.00.255.255
 # any

 Deny
 # 255.255.255.255
 # any

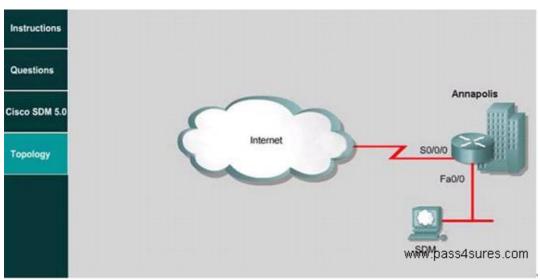
 Deny
 # 0.0.0.0
 # any

 Deny
 # any
 # any
 Service Log Option Description C Log Applications Description Real Time Streaming Protocol Extended SMTP SQL Net Protocol StreamWorks Protocol Alert Application Protocol . realaudio rtsp esmtp sqlnet streamworks 2 6 Apply Changes Discard Changes www.pass4sures.com Firewall and ACL 14:29:26 UTC Mon Nov 13 2006 🙆

Cisco 642-825: Practice Exam



Home	Configure Moni	tor Refresh	Save Search	? Help		Eisco Sviti
Tasks	C Firewall and ACL	Tuncan	Save Search	Theip		ALCO PARTICULAR
-	Create Firewall Edit Firewall	Policy / ACL Applic	ation Security			
terfaces and	Select a direction From:	FastEthernet0/0	WEL TO: S	erial0/0/0	· Ct Go	View Option
WHE ACL	Originating traffic • Returning traffic	+	FastEthernet0/0	Serial		
100	Firewall Feature Availability:		ewall : Active (From Access Rule: 10		 Inspection Ru 	e: SDM LOW
curity Audit	Services		L Cut Ra Copy	the second s	Serial0/0/0 - inbound	· Michool / Fann
Routing NAT	Action Source ☑ Deny ⇒ 172.16.0.00 ☑ Deny ⇒ 192.168.0.00 ☑ Deny ⇒ 192.168.0.00 ☑ Deny ⇒ 192.168.0.00 ☑ Deny ⇒ 192.525.255.255.00 ☑ Deny ⇒ 0.0.0 ☑ Deny ★ any	0.0.255.255 🛪 ar 55.255.255 🛪 ar		ice Li ip ip ip ip	xg Option	Description
1	•					
tion Prevention	Applications		Add - 🖬 E	and the second se	Global Settings	Summary Detail
-	Application Protocol	Alert	Audit Trail	Timeout	Description extended SMTP	
ity of Service	sqlnet streamworks ttp tcp				SQL Net Protocol StreamWorks Prot TFTP Protocol Transmission Cont User Datagram Pro	rol Protocol
NAC NAC	udp		-			



Off Shore Industries is a large worldwide sailing charter. The company has recently upgraded its Internet connectivity. As a recent addition to the network engineering team, you have been tasked with documenting the active Firewall configurations on the Annapolis router using the Cisco Router and Security Device Manager (SDM) utility. Using the SDM output from Firewall and ACL Tasks under the Configure tab, answer the following questions:

Which two statements would be true for a permissible incoming TCP packet on an untrusted Interface in this configuration? (Choose two.)

- A. The session originated from a trusted Interface
- B. The application is not specified within the inspection rule SDM_LOW.
- C. The session originated from an untrusted interface
- D. The packet has a source address of 10.79.233.186
- E. The packet has a source address of 172.16.81.108
- F. The packet has a source address of 198.133.219.135

Answer: A,F

Explanation:

According to the question, after configuring CBAC, the TCP traffic on the untrusted interface can be divided into two types: 1. The inspected return traffic from the intranet is permitted by the state table, so C is right. 2. The TCP traffic permitted by the ACL comes from external network, so E is right.

creat	e Firewal	Edit Firewall I	Policy / ACL	Application Security	NP					
Sele	ect a direc	tion From	FastEthemet0	io ,)段,	to: Serial0.0.0		EL Go		View Op	tion
		phating traffic		FastEthernet	s s	erial0/0/0	1	-	+	
				IOS Firewall - Active	(From EastEtherne	HD 0 to Set	(00.00)			
E	ewall Fea	ture Availability:		IOS Firewall : Active	and the second se	An Index of the local data		Rule:	SDM_LOW)	
	ewalt Fea	dure Availability:	Available	and the second se	100		Contraction of the local division of the loc	10.0	SDM_LOW)	
225	rvices	ture Availability. Source	Available	Access Rule	100		C Inspection	bound	and the second second second	0.000

The direction of ACL101 is from S0/0/0 to f0/0, which only allows the echo- reply/ icmp, timeexceede, unreachable services of the destination address of 172.16.81.108, denies any IP data packets from 0.0.0.0/8, 10.0.0.0/8, 127.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 224.0.0.0/4, 240.0.0.0/4 and 10.79.223/24, as well as adds log to any access. As to the address 172.16.81.108, only part of the ICMP packets are allowed. The address 198.133.219.135 is first initiated from the inside network. If an address of 198.133.219.135 is received from the outside network it should be directely dropped.

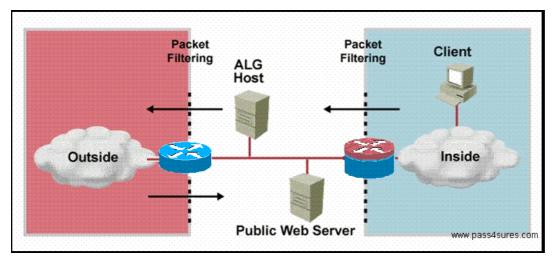
reat	e Firewall	Edit Firewall	Policy / ACL	Application S	ecurity		
Sele	ect a direct	tion From:	FastEtherne	•0.0	To: Senal0.0.0	- 12, Go	View Option
				FastEt	hernet0/0	Serial0/0/0	
	Orig	pinating traffic		17		SEC.	
	• Retu	urning traffic	+				
				LOO PLANT	And International Andrews		
				IOS Firewall ;	Active (From FastEthe	metolo to Senal0/0/0)	
Ek	rewall Fea	ture Availability	Available			metoro to Senatoro() Inspectio	n Rule: SDM_LOW
100	rewall Fea	ture Availability	Available	The Acces			and the second of the second sec
Se	Action	Source	- Add -	E Acces E Edit X.C Destination	s Rule: 101	O. Inspectio	and the second se
100	Action Denv	Source	- bbA -	Edit X C Destination	s Rule: 101 ut Ra Copy Ra	 Inspection Serial:0/0/0 - Inbour 	nd 🔹 🤹 🕼 Auszly Fleewo
Se	Action Deny	Source	- Add -	E Acces E Edit X.C Destination	s Rule: 101 ut Ra Copy Ra	 Inspection Serial:0/0/0 - Inbour 	nd • / dt Aus// Elemo Description
Se DO	Action Denv	Source 172.10.0.00 192.168.0.0	• Add • 10.200.400 0.0.255.255 255.255.255	Edit X.C Destination X dry X any	s Rule: 101 ut Ra Copy Ra	 Inspection Serial:0/0/0 - Inbour 	nd • / dt Aus// Elemo Description

QUESTION NO: 4

Refer to the exhibit. What is the name given to the security zone occupied by the public web server?

Cisco 642-825: Practice Exam





- A. proxy network
- B. ALG
- C. DMZ
- D. multiple DMZs
- E. extended proxy network
- F. protected subnet

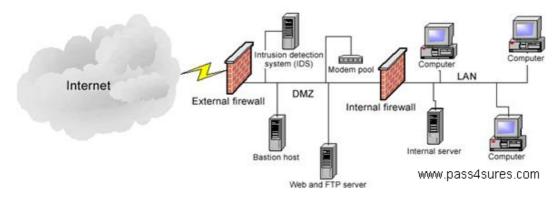
Answer: C

Explanation:

A DMZ, short for demilitarized zone, is a computer or small subnetwork that sits between a trusted internal network, such as a corporate private LAN, and an untrusted external network, such as the public Internet.

Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers. The term comes from military use, meaning a buffer area between two enemies.

A DMZ is the most common and secure firewall topology. It is often referred to as a screened subnet. A DMZ creates a secure space between your Internet and your network, as shown in the figure below:



QUESTION NO: 5



Refer to the exhibit. What are the two options that are used to provide High Availability IPsec? (Choose two.)

crypto map mymap 1 ipsec-isakmp set peer 10.1.1.1 reverse-route set transform-set esp-3des-sha match address 102

Interface FastEthernet 0/0 ip address 192.168.0.2 255.255.255.0 standby name group1 standby ip 192.168.0.3 crypto map mymap redundancy group1

access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0 0.0 0.255.255

- A. IPsec Stateful Switchover (SSO)
- B. Dynamic Crypto Map
- C. IPsec Backup Peerings
- D. Dual Router Mode (DRM) IPsec
- E. RRI
- F. HSRP

Answer: E,F

Explanation:

Reverse route injection (RRI) is the ability for static routes to be automatically inserted into the routing process for those networks and hosts protected by a remote tunnel endpoint. These protected hosts and networks are known as remote proxy identities. This is configured using the "reverse-route" command.

The Hot Standby Router Protocol (HSRP) provides network redundancy for IP networks, ensuring that user traffic immediately and transparently recovers from first hop failures in network edge devices or access circuits. This is done by logically grouping one or more routers into a single virtual gateway, and HSRP is configured using the "standby" configuration commands.

QUESTION NO: 6

What are three options for viewing Security Device Event Exchange (SDEE) messages in Security Device Manager (SDM)? (Choose three.)



- A. to view SDEE status messages
- B. to view SDEE actions
- C. to view SDEE statistics
- D. to view SDEE alerts
- E. to view SDEE keepalive messages
- F. to view all SDEE messages

Answer: A,D,F

Explanation:

SDEE Messages

This window lists the SDEE messages received by the router. SDEE messages are generated when there are changes to Cisco IOS IPS configuration.

SDEE Messages

Choose the SDEE message type to display:

All- SDEE error, status, and alert messages are shown.

Error-Only SDEE error messages are shown.

Status-Only SDEE status messages are shown.

Alerts-Only SDEE alert messages are shown.

Reference:

http://www.cisco.com/en/US/docs/routers/access/cisco_router_and_security_device_manager/24/software/user/guide/IPS.html#wp1083698

QUESTION NO: 7

Refer to the exhibit. What Cisco feature generated the configuration?