Cisco CCNA Security

Exam 210-260

Implementing Cisco Network Security

Questions No. 1
Refer to the exhibit

```
tacacs server tacacs1
   address ipv4 1.1.1.1
   timeout 20
   single-connection

tacacs server tacacs2
   address ipv4 2.2.2.2
   timeout 20
   single-connection

tacacs server tacacs3
   address ipv4 3.3.3.3
   timeout 20
   single-connection
```

Which statement about the given configuration is true?

A. The single-connection command causes the device to establish one connection for all TACACS transactions.
B. The single-connection command causes the device to process one TACACS request and then move to the next server.
C. The timeout command causes the device to move to the next server after 20 seconds of TACACS inactivity.
D. The router communicates with the NAS on the default port, TCP 1645

Answer: A

نرجع من ال output انه في كل اعداد ال Tacacs server يوجد (Single-connection)
او ان الجهاز سوف يكون Single-connection مثل ال Tacacs+ Server

Question No : 2
Refer to the exhibit.

```
dst          src        state     conn-id    slot
10.10.10.2   10.1.1.5   QM_IDLE   1          0
```

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command What does the given output show?

A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5.
B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5.
C. IPSec Phase 1 is down due to a QM_IDLE state.
D. IPSec Phase 2 is down due to a QM_IDLE state.

Answer: A

من ال conn-id نعرف انه Isec Phase 1 لعملية الربط بين 10.10.10.2 / 10.1.1.5

Question No : 3
In which two situations should you use in-band management? (Choose two.)

A. when management applications need concurrent access to the device
B. when you require administrator access from multiple locations
C. when a network device fails to forward packets
D. when you require ROMMON access
E. when the control plane fails to respond

Answer: A,B

ان ال In-band management معنى انه يمكن عمل ال management للجهاز عن طريق ال SSH او telnet من داخل الشبكة او خارجها ويعدة اتصالات

Concurrent → متزامن

fact
AB ← صحيح
AB

Question No : 4

Which type of PVLAN port allows a host in the same VLAN to communicate only with promiscuous hosts?

A. Community host in the PVLAN
B. Isolated host in the PVLAN
C. Promiscuous host in the PVLAN
D. Span for host in the PVLAN

Answer: B

- Isolated host inthe PVLAN

Question No : 5

Which type of layer 2 attack enables the attacker to intercept traffic that is intended for one specific recipient?

A. BPDU attack
B. DHCP Starvation
C. CAM table overflow
D. MAC address spoofing

Answer: D

كما نعرف ان ال MAC address spoofing تعني ان ال attacker يغير mac address
خاص ب client معين ليسرقه. حيث يمكنه استلام [illegible] البيانات
القادمة لهذا ال client.

Question No : 6

Which command initializes a lawful intercept view?
A. username cisco1 view lawful-intercept password cisco
B. parser view cisco li-view
C. li-view cisco user cisco1 password cisco
D. parser view li-view inclusive

Answer: C

لعمل ال lawful intercept/view يتم بواسطة الأمر التالي

#li-view li-password user username password password

او it will be

li-view cisco user cisco1 password cisco

Question No : 7

In which stage of an attack does the attacker discover devices on a target network?
A. Reconnaissance
B. Covering tracks
C. Gaining access
D. Maintaining access

Answer: A

Reconnaissance هو discovery process يستخدم لإيجاد معلومات عن الشبكة - حيث ان هذا البحث يمكن ان يتم من خلاله معرفة معلومات مثل ال IP addresses الأجهزة المتصلة بالشبكة ويمكن ان تجيب وايضاً يمكن معرفة ال Ports التي تكون مفتوحة في هذا الجهاز.

Question No : 8
You want to allow all of your company's users to access the Internet without allowing other Web servers to collect the IP addresses of individual users. What two solutions can you use? (Choose two).

A. Configure a proxy server to hide users' local IP addresses.
B. Assign unique IP addresses to all users.
C. Assign the same IP address to all users.
D. Install a Web content filter to hide users' local IP addresses.
E. Configure a firewall to use Port Address Translation.

Answer: A,E

proxy server :- وهو server ويكون hardware او software يستخدم لمنع الـ web servers من تجميع IPaddresses الـ users الخاصة بهم

- يستخدم الـ PAT في الـ firewall والبوابات لـ traffic.

Question No : 9
When a company puts a security policy in place, what is the effect on the company's business?

A. Minimizing risk
B. Minimizing total cost of ownership
C. Minimizing liability
D. Maximizing compliance

Answer: A

ان الـ security policy تستخدم لتقليل الخطر على الشبكة

Question No : 10

In a security context, which action can you take to address compliance?

A. Implement rules to prevent a vulnerability.
B. Correct or counteract a vulnerability.
C. Reduce the severity of a vulnerability.
D. Follow directions from the security appliance manufacturer to remediate a vulnerability.

Answer: A

ان ال compliance تعني تطبيق ال security policy على الشبكة والغاية
الاساسية هي لتجنب الاختراقات والثغور .

Q# what do you do when you have a network object or group and want to use an Ip address

- Dynamic NAT

Question No : 11

Which two NAT types allows only objects or groups to reference an IP address? (choose two)

A. dynamic NAT
B. dynamic PAT
C. static NAT
D. identity NAT

Answer: A,C

في ال dynamic NAT او static NAT نحدد مجموعة او IP واحد لكي يخرج
ال النت ب Ip address واحد مثلا static NAT او مجموعة Ipaddress مثل ال dynamic NAT
١٠٠٪ كلاهم

واذا اضطر ولو تختار dynamic NAT

- dynamic NAT
- static NAT

Question No : 12

In which configuration mode do you configure the ***ip ospf authentication-key 1*** command?

A. Interface
B. routing process
C. global
D. privileged

Answer: A

R(conf-if)# IP ospf authentication-key 1

tut

A

A ← صحيح

Question No : 13

Which IOS command do you enter to test authentication against a AAA server?

A. dialer aaa suffix <suffix> password <password>
B. ppp authentication chap pap test
C. aaa authentication enable default test group tacacs+
D. test aaa-server authentication dialergroup username <user> password.

Answer: D

test aaa-server authentication dialergroup username <user> password

* في هذا الامر نتأكد من كيفية دخول الـ host مثلا وإعطاء الـ username و Password
هل سوف ينجح في الـ authentication مع الـ aaa server

tat

D ← صحيح

Question No : 14
Refer to the exhibit.

```
Router#show crypto ipsec sa
interface: FastEthernet0
Crypto map tag: SDM_CMAP_1, local addr 172.17.1.1
protected vrf: (none)
   local ident (addr/mask/prot/port): (10.40.20.0/255.255.255.0/0/0)
   remote ident (addr/mask/prot/port): (10.50.30.0/255.255.255.0/0/0)
   current_peer 192.168.1.1 port 500
   PERMIT, flags={origin_is_acl,}

   #pkts encaps: 68, #pkts encrypt: 68, #pkts digest: 68
   #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
```

For which reason is the tunnel unable to pass traffic?

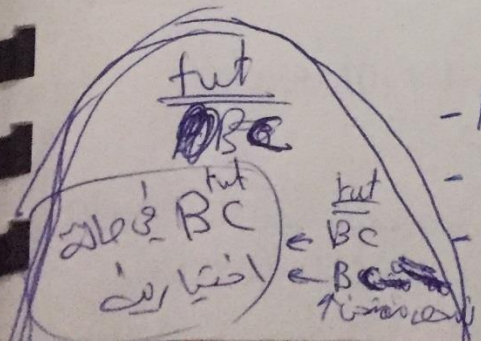
A. UDP port 500 is blocked.
B. The IP address of the remote peer is incorrect.
C. The tunnel is failing to receive traffic from the remote peer.
D. The local peer is unable to encrypt the traffic.

Answer: C

من السطر الاخير نوصف ان ال tunnel فشلت في ايصال اي traffic من ال remont Peer

Question No : 15
Which three statements are characteristics of DHCP Spoofing? (choose three)
A. Arp Poisoning
B. Modify Traffic in transit
C. Used to perform man-in-the-middle attack
D. Physically modify the network gateway
E. Protect the identity of the attacker by masking the DHCP address
F. can access most network devices
Answer: A,B,C

* في حالة اختيارت فقط ABC نختار



DHCP Spoofing خصائص ال

- ARP Poisoning
- modify traffic in transit
- used to perform man-in-the-middle attack

Question No : 16
What hash type does Cisco use to validate the integrity of downloaded images?

A. Sha1
B. Sha2
C. Md5
D. Md1

Answer: C

-MD5

Question No : 17
Refer to the exhibit.

dst	src	state	conn-id	slot
10.10.10.2	10.1.1.5	MM_NO_STATE	1	0

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

A. IKE Phase 1 main mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
B. IKE Phase 1 main mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.
C. IKE Phase 1 aggressive mode was created on 10.1.1.5, but it failed to negotiate with 10.10.10.2.
D. IKE Phase 1 aggressive mode has successfully negotiated between 10.1.1.5 and 10.10.10.2.

Answer: A

من الرسم نلاحظ انه phase 1 وتم انشاءه في 10.1.1.5 لـ
ب 10.10.10.2 لكن عملية المفاوضات فشلت

* (IKE) Internet key Exchange :- هو بروتوكول وظيفته نقل الـ policy وعملية الـ negotiation بين الراوترات وتبليغ الجهة الاخرى بالعمل بأدوات التشفير والـ authentication وما الى ذلك لكي يعمل الراوترين على نفس البروتوكولات

ترتيب السؤال 12

Question No : 18
What configure mode you used for the command ip ospf authentication-key cisco?

A. global
B. privileged
C. in-line
D. Interface

Answer: D

Question 12

In which configuration mode do you configure the IP ospf authentication-key command

A - Interface
B - Routing process
C - global
D - Privileged

Answer :- A

Question No : 19
Which option is a characteristic of the RADIUS protocol?

A. uses TCP
B. offers multiprotocol support
C. combines authentication and authorization in one process
D. supports bi-directional challenge

Answer: C

RADIUS يجمع بين ال authentication و ال authorization في process واحد

Question No : 20

Which of the following statements about access lists are true? (Choose three.)

A. Extended access lists should be placed as near as possible to the destination
B. Extended access lists should be placed as near as possible to the source
C. Standard access lists should be placed as near as possible to the destination
D. Standard access lists should be placed as near as possible to the source
E. Standard access lists filter on the source address
F. Standard access lists filter on the destination address

Answer: B,C,E

- Extended Acl تكون قريبة من ال Source (*)
- Standard Acl تكون قريبة من ال destination
- Standard Acl تستخدم ال Source address كعنوان لل Packet وتعمل
ل filtering على اساس ال Source address لل Packet

Question No : 21

Which description of the nonsecret numbers that are used to start a Diffie-Hellman exchange is true?

A. They are large pseudorandom numbers.
B. They are very small numbers chosen from a table of known values
C. They are numeric values extracted from hashed system hostnames.
D. They are preconfigured prime integers

Answer: D

- they are preconfigured prime integers

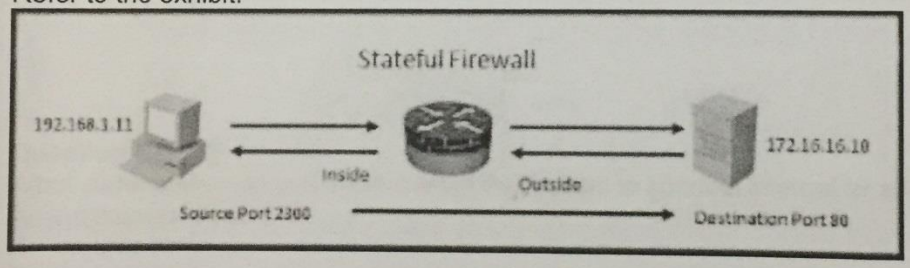
Question No : 22
What is a valid implicit permit rule for traffic that is traversing the ASA firewall?

A. ARPs in both directions are permitted in transparent mode only.
B. Unicast IPv4 traffic from a higher security interface to a lower security interface is permitted in routed mode only.
C. Unicast IPv6 traffic from a higher security interface to a lower security interface is permitted in transparent mode only.
D. Only BPDUs from a higher security interface to a lower security interface are permitted in transparent mode.
E. Only BPDUs from a higher security interface to a lower security interface are permitted in routed mode.

Answer: A

ان الـ ARPs يسمح لها بالمرور في الـ firewall بكل الاتجاهين لكن في حالة كان الـ firewall بحالة transparent mode فقط

Question No : 23
Refer to the exhibit.



Using a stateful packet firewall and given an inside ACL entry of permit ip 192.16.1.0 0.0.0.255 any, what would be the resulting dynamically configured ACL for the return traffic on the outside ACL?
A. permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300
B. permit ip 172.16.16.10 eq 80 192.168.1.0 0.0.0.255 eq 2300
C. permit tcp any eq 80 host 192.168.1.11 eq 2300
D. permit ip host 172.16.16.10 eq 80 host 192.168.1.0 0.0.0.255 eq 2300

Answer: A

[redacted] في الـ intercept بيوقع السماح للسيرفر فقط الى الـ PC كجواب الـ request وتكون كالتالي

permit tcp host 172.16.16.10 eq 80 host 192.168.1.11 eq 2300

Question No : 24

which port should (or would) be open if VPN NAT-T was enabled

A. port 500
B. port 500 outside interface
C. port 4500 outside interface
D. port 4500 ipsec

Answer: D

VPN NAT-T يجب ان يكون مفتوح عند تفعيل ال Port 4500 Ipsec ان ال

conceal → اخفاء

Question No : 25
What command could you implement in the firewall to conceal internal IP address?
A. no source-route
B. no broadcast....
C. no proxy-arp

Answer: C

- No proxy-arp

Act
C
C → متشابه

Question No : 26
Which aaa accounting command is used to enable logging of the start and stop records for user terminal sessions on the router?

A. aaa accounting network start-stop tacacs+
B. aaa accounting system start-stop tacacs+
C. aaa accounting exec start-stop tacacs+
D. aaa accounting connection start-stop tacacs+
E. aaa accounting commands 15 start-stop tacacs+

Answer: C

aaa accounting exec start-stop tacacs+

tut
C
C

Question No : 27

Which quantifiable item should you consider when your organization adopts new technologies?
A. threats
B. vulnerability
C. risk
D. exploits

Answer: C

Risk

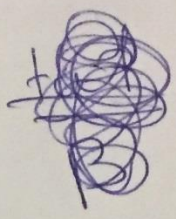
tut
C
C
C

Question No : 28
Which type of IPS can identify worms that are propagating in a network?

A. Policy-based IPS
B. Anomaly-based IPS
C. Reputation-based IPS
D. Signature-based IPS

Answer: B

Anomaly-based IPS



Question No : 29

Which prevent the company data from modification even when the data is in transit?
A. Confidentiality
B. Integrity
C. Vailability

Answer: B

الـ Integrity هي اننا نتأكد من الـ data لازم تتغير
خلال الارسال او داخل الانترنت

Question No : 30
Protocols supported in contest aware VRF over VRF lite? (Choose Two)

A. EIGRP
B. Multicast
C. CGR

Answer: A,B

الـ VRF over VRF lite بتدعم ان

- EIGRP
- Multicast

fact
AB

Question No : 31
Which two next-generation encryption algorithms does Cisco recommend? (Choose two.)
A. AES
B. 3DES
C. DES
D. MD5
E. DH-1024
F. SHA-384

Answer: A,F

الـ next-gen encryption بتدعم Cisco ان

- AES
- SHA-384

Question No : 32
What is one requirement for locking a wired or wireless device from ISE?

A. The ISE agent must be installed on the device.
B. The device must be connected to the network when the lock command is executed.
C. The user must approve the locking action.
D. The organization must implement an acceptable use policy allowing device locking.

Answer: A

Question No : 33
Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header

Answer: D,E,F

- Pad length
- next header

transmission encryption ESP fields

- Padding
- Pad length
- Next Header

Question No : 34
With which preprocesor do you detect incomplete TCP handshakes?

A. rate based prevention
B. portscan detection

Answer: A

Question what type of Diffie-hellman group would you expect to be utilized on a wireless device?

A - Group 4
B - Group 7
C - Group 5
D - Group 3

- group 7

tut
B

Answer B

Question No : 35
Which option is the default value for the Diffie-Hellman group when configuring a site-to site VPN on an ASA device?

A. Group 1
B. Group 2
C. Group 5
D. Group 7

Answer: B

- group 2

tut
B ← ciao

Question which of the Diffie-Hellman group are support by CISCO VPN product (Choose all that apply)

A - group 1
B - group 2
C - group 3
D - group 5
E - group 7
F - group 8
G - group 9

- group 1
- group 2
- group 5
- group 7

tut
A B D E
A B D E
A B D E
A B D E

Question No : 36
Refer to the exhibit

```
Oct 13 19:46:06.170: AAA/MEMORY: create_user (0x4C5E1F60) user='tecteam'
ruser='NULL' ds0=0 port='tty515' rem_addr='10.0.2.13' authen_type=ASCII
service=ENABLE priv=15 initial_task_id='0', vrf= (id=0)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): port='tty515' list=''
action=LOGIN service=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): console enable - default to
enable password (if any)
Oct 13 19:46:06.170: AAA/AUTHEN/START (2600878790): Method=ENABLE
Oct 13 19:46:06.170: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): continue_login
(user='(undef)')
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = GETPASS
Oct 13 19:46:07.266: AAA/AUTHEN/CONT (2600878790): Method=ENABLE
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): password incorrect
Oct 13 19:46:07.266: AAA/AUTHEN (2600878790): status = FAIL
Oct 13 19:46:07.266: AAA/MEMORY: free_user (0x4C5E1F60) user='NULL'
ruser='NULL' port='tty515' rem_addr='10.0.2.13' authen_type=ASCII service=ENABLE
priv=15 vrf= (id=0)
```

Which statement about this output is true?

A. The user logged into the router with the incorrect username and password.
B. The login failed because there was no default enable password.
C. The login failed because the password entered was incorrect.
D. The user logged in and was given privilege level 15.

Answer: C

فشل الدخول بسبب ان ال password خطأ

Question No : 37
What are two challenges faced when deploying host-level IPS? (Choose Two)

A. The deployment must support multiple operating systems.
B. It does not provide protection for offsite computers.
C. It is unable to provide a complete network picture of an attack.
D. It is unable to determine the outcome of every attack that it detects.
E. It is unable to detect fragmentation attacks.

Answer: A,B

Answer AC

- the deployment must support multiple operating systems
- ~~It does not provide protection for offsite computers~~.
- It is unable to provide a complete network picture of an attack

tut
AC
AC
AC
AC

elce
AB

Question No : 38
In which three cases does the ASA firewall permit inbound HTTP GET requests during normal operations? (Choose three).
A. when matching NAT entries are configured
B. when matching ACL entries are configured
C. when the firewall receives a SYN-ACK packet
D. when the firewall receives a SYN packet
E. when the firewall requires HTTP inspection
F. when the firewall requires strict HTTP inspection

Answer: A,B,D

elce (168.1.7.5)

- ~~when matching NAT entries are configured~~
- ~~when matching ACL entries are configured~~
- when the firewall receives a SYN packet

Question No : 39 Same as Q 33

Which three ESP fields can be encrypted during transmission? (Choose three.)

A. Security Parameter Index
B. Sequence Number
C. MAC Address
D. Padding
E. Pad Length
F. Next Header

Answer: D,E,F

- Padding
- Pad Length
- Next header

Question No : 40

Which two protocols enable Cisco Configuration Professional to pull IPS alerts from a Cisco ISR router? (Choose two.)

A. syslog
B. SDEE
C. FTP
D. TFTP
E. SSH
F. HTTPS

Answer: B,F

- SDEE
- HTTPS

tut
B F

Question No : 41
Which type of encryption technology has the broadest platform support to protect operating systems?

A. software
B. hardware
C. middleware
D. file-level

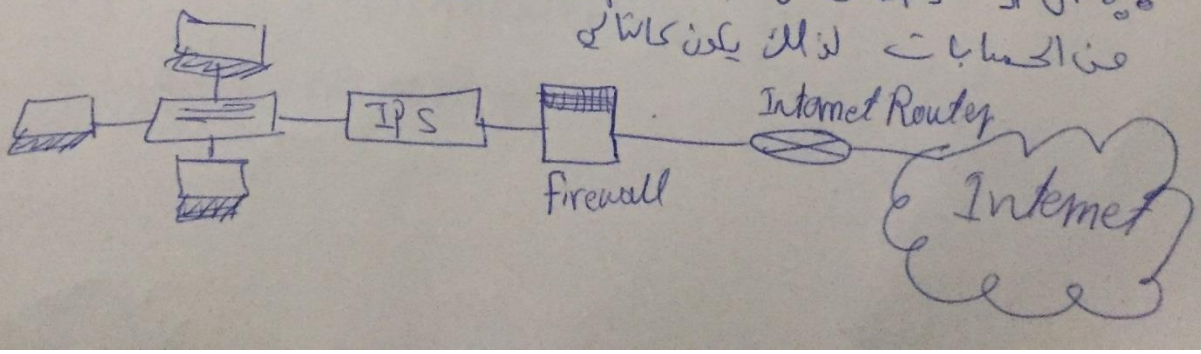
Answer: A

-Software

Question No : 42
Which option is the most effective placement of an IPS device within the infrastructure?
A. Inline, behind the internet router and firewall
B. Inline, before the internet router and firewall
C. Promiscuously, after the Internet router and before the firewall
D. Promiscuously, before the Internet router and the firewall

Answer: A

... ان الـ IPS تعمل inspection اكثر من الـ Firewall لذلك هي تعمل الحماية من الهجمات لذلك يكون كذلك



Question No : 43
An attacker installs a rogue switch that sends superior BPDUs on your network. What is a possible result of this activity?

A. The switch could offer fake DHCP addresses.
B. The switch could become the root bridge.
C. The switch could be allowed to join the VTP domain.
D. The switch could become a transparent bridge.

Answer: B

في حالة ان ال switch استلم superior BPDUs فأنه سوف تتحول الى ال root bridge

Question No : 44
Which two devices are components of the BYOD architectural framework?
A. Prime Infrastructure
B. Nexus 7010 Switch
C. Cisco 3945 Router
D. Wireless Access Points
E. Identity Services Engine

Answer: A,E

BYOD (Bring your own device) components
- Prime infrastructure
- Identity services engine

AE

Question No : 45
Which two characteristics apply to an Intrusion Prevention System (IPS) ?(Choose two)

A. Does not add delay to the original traffic.
B. Cabled directly inline with the flow of the network traffic.
C. Can drop traffic based on a set of rules.
D. Runs in promoscous mode.
E. Cannot drop the packet on its own

Answer: B,C

characteristics of IPS
- cabled directly inline with the flow of the network traffic
- can drop traffic based on a set of rules

tut
BC ← ignore
BC

Question No : 46
What configuration allows AnyConnect to automatically establish a VPN session when a user logs in to the computer?

A. always-on
B. proxy
C. transparent mode
D. Trusted Network Detection

Answer: A

always-on allows anyconnect to automatically establish a VPN when a user logs in the computer.

Question No : 47
When is the default deny all policy an exception in zone-based firewalls?
A. When traffic traverses two interfaces in in the same zone
B. When traffic terminates on the router via the self zone
C. When traffic sources from the router via the self zone
D. When traffic traverses two interfaces in different zones

Answer: A

(*) عندما ينتقل الـ traffic من interface الى interface اخر في نفس الـ Zone فانه لا تطبق عليه الـ Policy ويكون الـ default permit لـ traffic الـ ip

tut
A ← صحيح
A
A
A
A

Question No : 48
With which technology do apply integrity, confidentially and authenticate the source
A. IPSec
B. IKE
C. Certificate authority
D. Data encryption standards

Answer: A

ان الـ IPsec يدعم الـ
- Integrity
- Confidentiality
- authentication

tut
A ← صحيح

Question No : 49
Which two authentication types does OSPF support? (Choose two.)

A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES

Answer: A,B

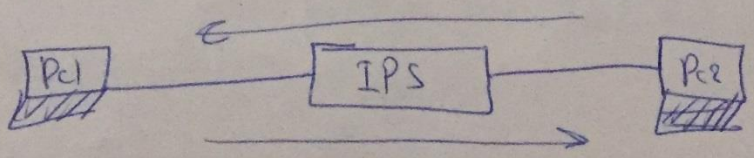
⊛ ان ال ospf بدعم في ال authentication

- Plaintext
- MD5

Question No : 50
Which IPS mode provides the maximum number of actions?
A. inline
B. promiscuous
C. span
D. failover
E. bypass

Answer: A

لان ال inline بكون كالتالي



حيث بمر ال traffic من خلال الجهاز ال IPS الاخير

Question No : 51
Which type of firewall can act on the behalf of the end device?

A. Stateful packet
B. Application
C. Packet
D. Proxy

Answer: D

ان ال application/proxy firewall يمكن ان تمثل client حيث تكون خلف application الـ firewall. لذلك اذا حاول الـ hacker واكتشف ثغرة في الـ (end device) client (PC) فانه سوف يظن ان الـ client ≤ proxy server

Question No : 52
What is the primary purpose of a defined rule in an IPS?

A. to configure an event action that takes place when a signature is triggered
B. to define a set of actions that occur when a specific user logs in to the system
C. to configure an event action that is pre-defined by the system administrator
D. to detect internal attacks

Answer: A

هو الصف من القواعد (القوانين) في الـ IPS

- to configure an event action that takes place when a signature is triggered

Question No : 53
Whitwhich type of Leyer 2 attack can you "do something" for one host:

A. MAC spoofing
B. CAM overflow....

Answer: A

ممكن ان يجيك في السؤال ما هو نوع ال attack الذي يستهدف host معين واحد

- MAC spoofing

Question No : 54
Which Sourcefire logging action should you choose to record the most detail about a connection?

A. Enable logging at the end of the session.
B. Enable logging at the beginning of the session.
C. Enable alerts via SNMP to log events off-box.
D. Enable eStreamer to log events off-box.

Answer: A

-Enable logging at the end of the session

Question No : 55
In which type of attack does an attacker send email messages that ask the recipient to click a link such as https://www.cisco.net.cc/securelogon?

A. phishing
B. pharming
C. solicitation
D. secure transaction

Answer: A

- phishing

Question No : 56
Which sensor mode can deny attackers inline?
A. IPS
B. fail-close
C. IDS
D. fail-open

Answer: A

- IPS

Question No : 58
Which statement about IOS privilege levels is true?

A. Each privilege level supports the commands at its own level and all levels below it.
B. Each privilege level supports the commands at its own level and all levels above it.
C. Privilege-level commands are set explicitly for each user.
D. Each privilege level is independent of all other privilege levels.

Answer: A

- Each privilege level supports the commands at its own level and all levels below it.

Question No : 59
In which three ways does the RADIUS protocol differ from TACACS? (Choose three.)
A. RADIUS uses UDP to communicate with the NAS.
B. RADIUS encrypts only the password field in an authentication packet.
C. RADIUS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.
D. RADIUS uses TCP to communicate with the NAS.
E. RADIUS can encrypt the entire packet that is sent to the NAS.
F. RADIUS supports per-command authorization.

Answer: A,B,C

- RADIUS uses UDP to communicate with the NAS
- RADIUS encrypts only the password field in authentication packet
- RADIUS authenticates and authorizes simultaneously, causing fewer packets to be transmitted.

Question No : 60
What VPN feature allows traffic to exit the security appliance through the same interface it entered?

A. hairpinning
B. NAT
C. NAT traversal
D. split tunneling

Answer: A

ان ال hair-pinning تسمح ال traffic بالخروج عن نفس ال interface
الذي دخلت منه

Question No : 61
Which feature of the Cisco Email Security Appliance can mitigate the impact of snowshoe spam and sophisticated phishing attacks?

A. contextual analysis
B. holistic understanding of threats
C. graymail management and filtering
D. signature-based IPS

Answer: A

- contextual analysis

tat
A ← جواب

Question No : 62
Diffie-Hellman key exchange question

A. IKE

Answer: A

-IKE

Question No : 63
Which NAT option is executed first during in case of multiple nat translations?

A. dynamic nat with shortest prefix
B. dynamic nat with longest prefix
C. static nat with shortest prefix
D. static nat with longest prefix

Answer: D

في حالة يوجد عدة انواع من الـ NAT، فأول نوع يتم تنفيذه هو ↓
- Static NAT with longest prefix

penetration → اختراق

Question No : 64

How can you detect a false negative on an IPS?

A. View the alert on the IPS.
B. Review the IPS log.
C. Review the IPS console.
D. Use a third-party system to perform penetration testing.
E. Use a third-party to audit the next-generation firewall rules.

Answer: D

false negative :- وهو ان يكون هناك attack ولكن الانذار التابع لل IPS لم يشتغل اي ان ال IPs لم يكتشف هذا ال attack

لحل هذه المشكلة يمكن ان نضع third-party او جهاز خارجي منل SNMP لتجميع مراقبة ال traffic وتشغيل الانذار في حالة حصول اي attack

Question No : 65

The command debug crypto isakmp results in ?
A. Troubleshooting ISAKMP (Phase 1) negotiation problems

Answer: A

Question No : 66
Which tool can an attacker use to attempt a DDoS attack?

A. botnet
B. Trojan horse
C. virus
D. adware

Answer: A

- botnet used for DDos attacks

Question No : 67

Which protocols use encryption to protect the confidentiality of data transmitted between two parties? (Choose two.)

A. FTP
B. SSH
C. Telnet
D. AAA
E. HTTPS
F. HTTP

Answer: B,E

- SSH
- HTTPS

firepower is Kind of firewall

Question No : 68

Which firepower preprocessor block traffic based on IP?

A. Signature-Based
B. Policy-Based
C. Anomaly-Based
D. Reputation-Based

Answer: D

ال ASA firepower بستخدم ال filter ال traffic بناءً على
Reputation-Based والمعلومة IPaddress
conditions

tut
D ← صح
D

Question No : 69

You have been tasked with blocking user access to websites that violate company policy, but the sites use dynamic IP addresses. What is the best practice for URL filtering to solve the problem?

A. Enable URL filtering and use URL categorization to block the websites that violate company policy.
B. Enable URL filtering and create a blacklist to block the websites that violate company policy.
C. Enable URL filtering and create a whitelist to block the websites that violate company policy.
D. Enable URL filtering and use URL categorization to allow only the websites that company policy allows users to access.
E. Enable URL filtering and create a whitelist to allow only the websites that company policy allows users to access.

Answer: A

- Enable URL filtering and use URL categorization to block the websites that Violate company policy

tut
A ← صح
A

Question No : 70
Which three options are common examples of AAA implementation on Cisco routers? (Choose three.)

A. authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
B. authenticating administrator access to the router console port, auxiliary port, and vty ports
C. implementing PKI to authenticate and authorize IPsec VPN peers using digital certificates
D. tracking Cisco NetFlow accounting statistics
E. securing the router by locking down all unused services
F. performing router commands authorization using TACACS+

Answer: A,B,F

- authenticating remote users who are accessing the corporate LAN through IPsec VPN connections
- authenticating administrator access to the router console port, auxiliary port, and vty ports
- performing router commands authorization using TACACS+

Question No : 72

Which command verifies phase 1 of an IPsec VPN on a Cisco router?

A. show crypto map
B. show crypto ipsec sa
C. show crypto isakmp sa
D. show crypto engine connection active

Answer: C

لـ IPsec VPN ال phase 1 هو الأمر

R#show crypto isakmp sa

show crypto isakmp sa ← phase 1
show crypto ipsec sa ← phase 2

Question No : 73
Refer to the exhibit.

```
current_peer: 10.1.1.5
   PERMIT, flags={origin_is_acl,}
  #pkts encaps: 1205, #pkts encrypt: 1205, #pkts digest 1205
  #pkts decaps: 1168, #pkts decrypt: 1168, #pkts verify 1168
  #pkts compressed: 0, #pkts decompressed: 0
  #pkts not compressed: 0, #pkts compr. failed: 0,
  #pkts decompress failed: 0, #send errors 0, #recv errors 0
   local crypto endpt.: 10.1.1.1, remote crypto endpt.: 10.1.1.5
```

While troubleshooting site-to-site VPN, you issued the show crypto ipsec sa command. What does the given output show?

A. IPSec Phase 2 is established between 10.1.1.1 and 10.1.1.5.
B. ISAKMP security associations are established between 10.1.1.5 and 10.1.1.1.
C. IKE version 2 security associations are established between 10.1.1.1 and 10.1.1.5.
D. IPSec Phase 2 is down due to a mismatch between encrypted and decrypted packets.

Answer: A

phase2 دايمًا Show crypto IPsec sa من الأمر

يعرض remote crypto endpoint و من Local crypto end point

10.1.1.5 و 10.1.1.1 تم انشاء بين IPSEC phase2 أن

Question No : 74
Which type of address translation supports the initiation of communications bidirectionally?

A. multi-session PAT
B. static NAT
C. dynamic PAT
D. dynamic NAT
~~**Answer: D**~~

Answer B

ان ال (Static NAT) تبقي الاتصال (translation) شغال لذلك تسمح للاتصال بأن يتم انشاءه بكلا الطرفين يعني ذلك اتصال من ال Real host الى Remotehost او بالعكس.

tut

B

B

ايضاً static NAT يعطي transparent model

Question No : 75
Which two features are supported in a VRF-aware software infrastructure before VRF-lite? (Choose two)
which protocol supported in context aware VRF over VRF-lite?
A. priority queuing
B. EIGRP
C. multicast
D. WCCP
E. fair queuing

Answer: B,C

ان VRF تدعم

- EIGRP
- multicast

Question No : 76
What are the three layers of a hierarchical network design? (Choose three.)

A. access
B. core
C. distribution
D. user
E. server
F. Internet

Answer: A,B,C

- access layer
- distribution layer
- core layer

Question No : 77
Which two characteristics of the TACACS+ protocol are true? (Choose two.)

A. uses UDP ports 1645 or 1812
B. separates AAA functions
C. encrypts the body of every packet
D. offers extensive accounting capabilities
E. is an open RFC standard protocol

Answer: B,C

- separates AAA functions
- encrypts the body of every packet

Question No : 78

Which two options are advantages of an application layer firewall? (Choose two.)

A. provides high-performance filtering
B. makes DoS attacks difficult
C. supports a large number of applications
D. authenticates devices
E. authenticates individuals

Answer: B,E

كما نعرف ان ال application layer firewall بتعمل inspection لحد ال
application layer لذلك of

- makes Dos attack difficult
لازم تفحص ال IP و ال port علشان تكشف ال DOS

- authenticates individuals

tut
BE
BE ← مضمون
BE

Question No : 79
Which ports need to be active for AAA server and a Microsoft server to permit Active Directory authentication?

A. 445 and 389
B. 888 and 3389
C. 636 and 4445
D. 363 and 983

Answer: A

445 & 389 port no.

tut
A
A
A
A ← مضمون

Question No : 80
Which source port does IKE use when NAT has been detected between two VPN gateways?

A. TCP 4500
B. TCP 500
C. UDP 4500
D. UDP 500

Answer: C

the encapsulation of IKE and ESP in UDP port 4500 enables these Protocols to pass through a device or firewall performing NAT

Question No : 81
The Oakley cryptography protocol is compatible with following for managing security?

A. IPSec
B. ISAKMP
C- port security

Answer: B

— IKE is a protocol that implements the Oakley key exchange and work with ISAKMP

(Inside of the internet security Association and key management Protocal "ISAKmp")

Question No : 82
Which Cisco Security Manager application collects information about device status and uses it to generate notifications and alerts?

A. FlexConfig
B. Device Manager
C. Report Manager
D. Health and Performance Monitor

Answer: D

-Health and Performance Monitor

حيث تستخدم لجمع معلومات حالة الـ devices وتولد الاشعارات
و انذار بناءً على المعلومات المراقبة

Question No : 84
Which feature allows a dynamic PAT pool to select the next address in the PAT pool instead of the next port of an existing address?

A. next IP
B. round robin
C. dynamic rotation
D. NAT address rotation

Answer: B

- Roud Robin

Question No : 85
Which countermeasures can mitigate ARP spoofing attacks? (Choose two.)

A. Port security
B. DHCP snooping
C. IP source guard
D. Dynamic ARP inspection

Answer: B,D

ARP spoofing attack يمنع هاي الطريقة

- DHCP snooping
- Dynamic ARP inspection

~~Question No : 86~~
~~Which IPS mode is less secure than other options but allows optimal network throughput?~~

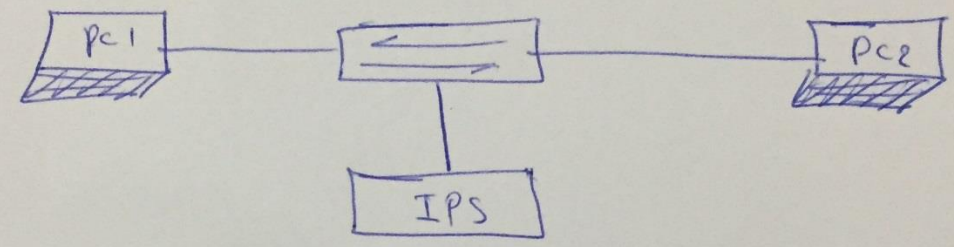
Question 86 :-

Which IPS mode is Less secure than other options but allows optimal network throughput?

A. promiscuous mode
B. inline mode
C. inline-bypass mode
D. transparent mode.

Answer: A

عملا نعرف ان الـ promiscuous mode في الـ IPS يكون كالتالي



من الـ topology نعرف انه ليس امن ولكنه لا يعطل سير السرعة لانها نسخة من البيانات ترسل له وليس في طريق الـ data

tut

A

A

Question No : 87
Which wildcard mask is associated with a subnet mask of /27?

A. 0.0.0.31
B. 0.0.027
C. 0.0.0.224
D. 0.0.0.255

Answer: A

Slash	subnetmask	Wildcard mask
/27	255.255.255.224	0.0.0.31

Question No : 88
Which statement about a PVLAN isolated port configured on a switch is true?

A. The isolated port can communicate only with the promiscuous port.
B. The isolated port can communicate with other isolated ports and the promiscuous port.
C. The isolated port can communicate only with community ports.
D. The isolated port can communicate only with other isolated ports.

Answer: A

Promiscuous port يستطيع ان يتعامل مع ال Isolated port كما نعرف ان ال
وال trunk ان وجد فقط

Question No : 89
Which IDS/IPS solution can monitor system processes and resources?

A. IDS
B. HIPS
C. PROXY
D. IPS

Answer: B

— HIPS

fut

B

B ← صحيح

B

Question No : 90
In which type of attack does the attacker attempt to overload the CAM table on a switch so that the switch acts as a hub?

A. MAC spoofing
B. gratuitous ARP
C. MAC flooding
D. DoS

Answer: C

كما نعلم ان ال MAC flooding هو attack حيث يقوم ال hacker بإغراق
ال switch بالكثير من ال packet وكل packet فيها source MAC address
يختلف . لذلك يقوم ال switch بتسجيل هذه العناوين في CAM table
الى ان يمتلئ ومن ثم يبدأ ال switch بمسح ال mac address القديمة
وعندما يريد user ان يرسل ال packet الى user آخر فان ال switch قد مسح
ال mac address لل users بسبب امتلاء ال CAM table . لذلك ان ال switch
لا يعلم موقع ال port لهذا ال mac لذلك تم ارسالها الى كل ال ports مثل ال hub

Question No : 91
Which product can be used to provide application layer protection for TCP port 25 traffic?

A. ESA
B. CWS
C. WSA
D. ASA

Answer: A

- ESA

Question No : 92
Which statement about Cisco ACS authentication and authorization is true?

A. ACS servers can be clustered to provide scalability.
B. ACS can query multiple Active Directory domains.
C. ACS uses TACACS to proxy other authentication servers.
D. ACS can use only one authorization profile to allow or deny requests.

Answer: A

authorization و authentication ال يمكن ان تجمع ال ACS servers

لتوفر [redacted] قابلية التوسع

نفس سؤال سابق

Question No : 93

Which two authentication types does OSPF support? (Choose two.)

A. plaintext
B. MD5
C. HMAC
D. AES 256
E. SHA-1
F. DES

Answer: A,B

OSPF support two authentication types
- plaintext
- MD5

Question No : 94

Refer to the exhibit.

```
authentication event fail action next-method
authentication event no-response action authorize vlan 101
authentication order mab dot1x webauth
authentication priority dot1x mab
authentication port-control auto
dot1x pae authenticator
```

If a supplicant supplies incorrect credentials for all authentication methods configured on the switch, how will the switch respond?

A. The supplicant will fail to advance beyond the webauth method.
B. The switch will cycle through the configured authentication methods indefinitely.
C. The authentication attempt will time out and the switch will place the port into the unauthorized state.
D. The authentication attempt will time out and the switch will place the port into VLAN 101.

Answer: A

يقول ماذا يحدث في حالة فشلت كل عمليات ال authentication
اي اصبحت down وهي كالتالي mab dot1x webauth
لذلك الكل صوان ال الجهاز سوف يفشل بالوصول الى الا مرحلة authentication
بعد ال Webauth .

Question No : 95
What is an advantage of implementing a Trusted Platform Module for disk encryption?

A. It provides hardware authentication.
B. It allows the hard disk to be transferred to another device without requiring re- encryption.dis
C. It supports a more complex encryption algorithm than other disk-encryption technologies.
D. It can protect against single points of failure.

Answer: A

كما تعرف ان ال Trusted platform modul لتوفير ال authentication

نفس سؤال سابق

Question No : 96
Which three statements describe DHCP spoofing attacks? (Choose three.)

A. They can modify traffic in transit.
B. They are used to perform man-in-the-middle attacks.
C. They use ARP poisoning.
D. They can access most network devices.
E. They protect the identity of the attacker by masking the DHCP address.
F. They are can physically modify the network gateway.

Answer: A,B,C

كما قلنا ان ال DHCP spoofing هو ان يستغل ال hacker ال DHCP الملك
ممكن ان يعطي ال pc يعطيه IP address في Subnet مختلفة. وممكن
ان يعطيه ال IP address خاطئة كـ Gateway لذلك تذهب له المعلومات عندما نريد
ارسالها الى ال Internet او الشبكات الاخرى. لذلك هو ممكن ان يتحكم
بالبيانات وايضا هذا هو man-in-the-middel-attack حيث يراقب البيانات
المرسلة و المستلمة لهذا ال AC . وايضا يستطيع

Question No : 97
What are purposes of the Internet Key Exchange in an IPsec VPN? (Choose two.)

A. The Internet Key Exchange protocol establishes security associations
B. The Internet Key Exchange protocol provides data confidentiality
C. The Internet Key Exchange protocol provides replay detection
D. The Internet Key Exchange protocol is responsible for mutual authentication

Answer: A,D

IKE protocol used to establish secured site-to-site VPN or remote access VPN and also used to negotiate for authentication

Question No : 98
What is the best way to confirm that AAA authentication is working properly?

A. Use the test aaa command.
B. Ping the NAS to confirm connectivity.
C. Use the Cisco-recommended configuration for AAA authentication.
D. Log into and out of the router, and then check the NAS authentication log.

Answer: A

الطريقة الأفضل لتأكد من ان aaa authentication يعمل بشكل صحيح هي
(test aaa command) الأمر

test aaa-server authentication dielangroup username <user> password

tut
A

Question No : 99
Refer to the exhibit.

```
crypto ipsec transform-set myset esp-md5-hmac esp-aes-256
```

What are two effects of the given command? (Choose two.)

A. It configures authentication to use AES 256.
B. It configures authentication to use MD5 HMAC.
C. It configures authorization use AES 256.
D. It configures encryption to use MD5 HMAC.
E. It configures encryption to use AES 256.

Answer: B,E

authentication encryption

Crypto IPsec transform-set myset esp-md5-hmac esp-aes-256

Question No : 100
You have implemented a Sourcefire IPS and configured it to block certain addresses utilizing Security Intelligence IP Address Reputation. A user calls and is not able to access a certain IP address. What action can you take to allow the user access to the IP address?

A. Create a whitelist and add the appropriate IP address to allow the traffic.
B. Create a custom blacklist to allow the traffic.
C. Create a user based access control rule to allow the traffic.
D. Create a network based access control rule to allow the traffic.
E. Create a rule to bypass inspection to allow the traffic.

Answer: A

في حالة تريد ان تسمح ل user بالوصول الى عناوين ممنوع
الوصول اليها يمكن ان تكون
whitelest وتضع ال IPaddress ال user بها
لكي يتم السماح لهذا ال user المحدد بالوصول الى هذه
IPaddresses ال

Question No : 101
Refer to the exhibit.

```
Username Engineer privilege 9 password 0 configure
Username Monitor privilege 8 password 0 watcher
Username HelpDesk privilege 6 password help
Privilege exec level 6 show running
Privilege exec level 7 show start-up
Privilege exec level 9 configure terminal
Privilege exec level 10 interface
```

Which line in this configuration prevents the HelpDesk user from modifying the interface configuration?

A. Privilege exec level 9 configure terminal
B. Privilege exec level 10 interface
C. Username HelpDesk privilege 6 password help
D. Privilege exec level 7 show start-up

Answer: A

في العودة اعلاه نلاحظ ان الـ help disk user لديه privilege level 6 فقط ونلاحظ ان الـ users في الـ privilege level 6 يستطيع تنفيذ امر show running ولا يستطيع التعديل على الاعدادات. لذلك ان privilege exec level 9 configure terminal هو الذي يمنع الـ help disk من التعديل على الاعدادات

Question No : 102
What IPSec mode is used to encrypt traffic between a server and VPN endpoint?

A. tunnel
B. Trunk
C. Aggregated
D. Quick
E. Transport

Answer: E

- transport mode

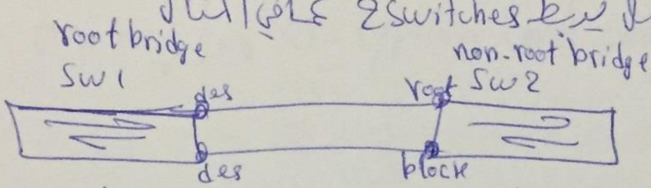
Question No : 103

When a switch has multiple links connected to a downstream switch, what is the first step that STP takes to prevent loops?

A. STP elects the root bridge
B. STP selects the root port
C. STP selects the designated port
D. STP blocks one of the ports

Answer: A

– عندما يوجد اكثر من كيبل يربط 2switches على المثال



فالـ STP ينتخب rootbridge ومن ثم ينفذ قوانين الـ STP
لتحديد الـ root port و designated ports و block port

Question No : 104

Which two functions can SIEM provide? (Choose Two)

A. Correlation between logs and events from multiple systems.
B. event aggregation that allows for reduced log storage requirements.
C. proactive malware analysis to block malicious traffic.
D. dual-factor authentication.
E. centralized firewall management.

Answer: A,C

– correlation between logs and events from multiple systems.

– Proactive malware analysis to block malicious traffic

tud
AC
Ac

Question No : 105
What mechanism does asymmetric cryptography use to secure data?

A. a public/private key pair
B. shared secret keys
C. an RSA nonce
D. an MD5 hash

Answer: A

asymmetric cryptography uses public/private key pair
means one key for encryption and another key for decryption

Question No : 106
Which three statements about Cisco host-based IPS solutions are true? (Choose three.)
A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behavior at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Answer: A,B,C

- It can view encrypted files
- It can have more restrictive policies than Network-based IPS
- It can generate alerts based on behavior at the desktop level.

Question No : 107
Referencing the CIA model, in which scenario is a hash-only function most appropriate?

A. securing wireless transmissions.
B. securing data in files.
C. securing real-time traffic
D. securing data at rest

Answer: D

-Securing data at rest

1st
D
B

Question Refering to CIA (confidentiality, Integrity, and availability), where would a hash-only make more sense

A - Data on File
B - Data at Rest

1st
B
B
B

Question No : 108
Which EAP method uses Protected Access Credentials?

A. EAP-FAST
B. EAP-TLS
C. EAP-PEAP
D. EAP-GTC

Answer: A

- EAP-FAST

Question No : 109
What is a reason for an organization to deploy a personal firewall?

A. To protect endpoints such as desktops from malicious activity.
B. To protect one virtual network segment from another.
C. To determine whether a host meets minimum security posture requirements.
D. To create a separate, non-persistent virtual environment that can be destroyed after a session.
E. To protect the network from DoS and syn-flood attacks.

Answer: A

ان ال personal firewall هو software يستخدم للسيطرة على layer3
و layer4 في الشبكة لذلك يستخدم لمنع اي فايروسات او
malicious في ال end point user

Question No : 110
Which type of security control is defense in depth?

A. Threat mitigation
B. Risk analysis
C. Botnet mitigation
D. Overt and covert channels

Answer: A

- threat mitigation

Question No : 111

In what type of attack does an attacker virtually change a device's burned-in address in an attempt to circumvent access lists and mask the device's true identity?

A. gratuitous ARP
B. ARP poisoning
C. IP spoofing
D. MAC spoofing

Answer: D

ان الـ burned-in address هو الـ mac address لذلك فان

mac spoofing هو attack يتم من خلاله استخدام الـ mac

ما الضحية في ارسال واستقبال الـ packets

Question No : 112

Which tasks is the session management path responsible for? (Choose three.)

A. Verifying IP checksums
B. Performing route lookup
C. Performing session lookup
D. Allocating NAT translations
E. Checking TCP sequence numbers
F. Checking packets against the access list

Answer: B,D,F

ان الـ ASA يفحص الـ packet من خلال access list وغيرها من الـ tasks لكي

يقرر هل سوف يمر الـ packet ام لا يمر . ولتنفيذ ذلك فانه اول packet

في الـ session سوف يمر من خلال الـ Session mangement path

وهو مسؤول عن التالي

- Performing route lookup
- Allocating NAT transulation
- Checking packets against the access list

Question No : 113
Which type of Cisco ASA access list entry can be configured to match multiple entries in a single statement?

A. nested object-class
B. class-map
C. extended wildcard matching
D. object groups

Answer: D

على اعتبار ان ال objectgroup ممكن ان تحتوي على عناوين عدة hosts.

Question No : 114
Which address block is reserved for locally assigned unique local addresses?

A. 2002::/16
B. FD00::/8
C. 2001::/32
D. FB00::/8

Answer: B

FD00::/8 is unique local IPv6 address

Question No : 115
Which type of mirroring does SPAN technology perform?

A. Remote mirroring over Layer 2
B. Remote mirroring over Layer 3
C. Local mirroring over Layer 2
D. Local mirroring over Layer 3

Answer: C

ان ال SPAN بيلقط ال switch layer2 (ports & VLANs)
في نفس ال switch بيلقط layer2 يعني ال Local mirroring over layer2

ا
اما ال RSPAN فانه بيلقط switch layer2 (ports & vlans)
في switch اخر بيعمل monitored device ان ال

Question No : 116
What VPN feature allows Internet traffic and local LAN/WAN traffic to use the same network connection?

A. split tunneling
B. hairpinning
C. tunnel mode
D. transparent mode

Answer: A

- split tunneling

Question No : 117
How can you proect CDP from reconnaissance attacks?

A. Enable dot1x on all ports that are connected to other switches.
B. Disable CDP on ports connected to endpoints.
C. Disbale CDP on trunk ports.
D. Enable dynamic ARP inspection on all untrusted ports.

Answer: B

- Disable CDP on ports connected to endpoints.

fut
B
B
B
B
B

Question No : 118
By which kind of threat is the victim tricked into entering username and password information at a disguised website?

A. Spoofing
B. Malware
C. Spam
D. Phishing

Answer: D

- phishing

Part 2

Question No : 119
Which statement about college campus is true?

A. College campus has geographical position.
B. College campus Hasn't got internet access.
C. College campus Has multiple subdomains.
D- college campus has very beautiful girls

Answer: A

- college campus has geogriphical position

fat
A

underlying → الأساسية

Question No : 120
Which statement is a benefit of using Cisco IOS IPS?

A. It uses the underlying routing infrastructure to provide an additional layer of security.
B. It works in passive mode so as not to impact traffic flow.
C. It supports the complete signature database as a Cisco IPS sensor appliance.
D. The signature database is tied closely with the Cisco IOS image.

Answer: A

- It uses underlying routing infrastructure to provide an additional layer of security.

.**Question No : 121**
After reloading a router, you issue the dir command to verify the installation and observe that the image file appears to be missing. For what reason could the image file fail to appear in the dir output?

A. The secure boot-image command is configured.
B. The secure boot-comfit command is configured.
C. The confreg 0x24 command is configured.
D. The reload command was issued from ROMMON.

Answer: A

#secure boot-image
this command enables or disables the securing of the running CISCO IOS Image
because this command has the effect of "hiding" the running image.

Question No : 122
Which statement about zone-based firewall configuration is true?

A. Traffic is implicitly denied by default between interfaces the same zone
B. Traffic that is desired to or sourced from the self-zone is denied by default
C. The zone must be configured before a can be assigned
D. You can assign an interface to more than one interface

Answer: C

- the zone must be configured before a can be assigned

tut
C ← ijao
C
C

Question No : 123
Which firewall configuration must you perform to allow traffic to flow in both directions between two zones?

A. You must configure two zone pairs, one for each direction.
B. You can configure a single zone pair that allows bidirectional traffic flows for any zone.
C. You can configure a single zone pair that allows bidirectional traffic flows for any zone except the self zone.
D. You can configure a single zone pair that allows bidirectional traffic flows only if the source zone is the less secure zone.

Answer: A

outside zone ... inside zone ... zone pair

- You must configure two zone pairs, one for each direction.

Question No : 124
A proxy firewall protects against which type of attack?

A. cross-site scripting attack
B. worm traffic
C. port scanning
D. DDoS attacks

Answer: A

eke
A

- cross-site scripting attack

Question No : 125
What can the SMTP preprocessor in FirePOWER normalize?

A. It can extract and decode email attachments in client to server traffic.
B. It can look up the email sender.
C. It compares known threats to the email sender.
D. It can forward the SMTP traffic to an email filter server.
E. It uses the Traffic Anomaly Detector.

Answer: A

- It can extract and decode email attachments in client to server traffic

Question No : 126
Which command help user1 to use enable,disable,exit&etc commands?

A. catalyst1(config)#username user1 privilege 0 secret us1pass
B. catalyst1(config)#username user1 privilege 1 secret us1pass
C. catalyst1(config)#username user1 privilege 2 secret us1pass
D. catalyst1(config)#username user1 privilege 5 secret us1pass

Answer: A

لما نشوف اوامر الـ enable , disable , exit ..... نلاقي privilege 0

- Catalyst1(config)# username user1 privilege 0 secret us1pass

Question No : 127
Which type of PVLAN port allows hosts in the same VLAN to communicate directly with each other?

A. community for hosts in the PVLAN
B. promiscuous for hosts in the PVLAN
C. isolated for hosts in the PVLAN
D. span for hosts in the PVLAN

Answer: A

- community for hosts in the PVLAN

* كما نعرف ان ال Community ports تستطيع التحدث مع ال community ports الاخرين وال promiscous port + trunk port

Question No : 128
How to verify that TACACS+ connectivity to a device?

A. You successfully log in to the device by using the local credentials.
B. You connect to the device using SSH and receive the login prompt.
C. You successfully log in to the device by using ACS credentials.
D. You connect via console port and receive the login prompt.

Answer: B

- You connect to the device using SSH and receive the login prompt

tut
B

Question No : 129

Which Cisco product can help mitigate web-based attacks within a network?

A. Adaptive Security Appliance
B. Web Security Appliance
C. Email Security Appliance
D. Identity Services Engine

Answer: B

- Web security Appliance used to mitigate web-based attack

Question No : 130

what causes a client to be placed in a guest or restricted VLAN on an 802.1x enabled network?

A. client entered wrong credentials multiple times.
B. client entered wrong credentials First time.

Answer: A

- Client entered wrong credential multiple times

تم وضع ال client في ال guest vlan او restricted vlan عند

يدخل معلومات الدخول عدة مرات بصورة خاطئة

tut

A

A

Question No : 131
If a switch port goes into a blocked state only when a superior BPDU is received, what mechanism must be in use?

A. STP root guard
B. EtherChannel guard
C. loop guard
D. STP BPDU guard

Answer: A

STP root guard

fut

A
A
A ← تمرين
A

Question No : 132
Which filter uses in Web reputation to prevent from Web Based Attacks? (Choose two)

A. outbreak filter
B. buffer overflow filter
C. bayesian overflow filter
D. web reputation
E. exploit filtering

Answer: A,D,E

else

- outbreak filter
- [illegible]
- exploit filtering

fut

A E
A E
A E

Question No : 133
What technology can you use to provide data confidentiality, data integrity and data origin Authentication on your network?

A. Certificate Authority
B. IKE
C. IPSec
D. Data Encryption Standards

Answer: C

IPsec can provide confidentiality, integrity, authentication

Question No : 134
What is an advantage of placing an IPS on the inside of a network?

A. It can provide higher throughput.
B. It receives traffic that has already been filtered.
C. It receives every inbound packet.
D. It can provide greater security.

Answer: B

- It receives traffic that has already been filtered

كما نعلم ان ال firewall يعمل filtering لل data ولكن ال IPS يعمل deep inspection للبيانات لذلك يتم وضعه بعد ال firewall.
لذلك ان ال IPS يستلم ال traffic الآمن اصلاً تم عمل filtering له بواسطة ال firewall

Question No : 135

Which line in the following OSPF configuration will not be required for MD5 authentication to work?

```
interface GigabitEthernet0/1
ip address 192.168.10.1 255.255.255.0
ip ospf authentication message-digest
ip ospf message-digest-key 1 md5 CCNA
!
router ospf 65000
router-id 192.168.10.1
area 20 authentication message-digest
network 10.1.1.0 0.0.0.255 area 10
network 192.168.10.0 0.0.0.255 area 0
```

A. ip ospf authentication message-digest
B. network 192.168.10.0 0.0.0.255 area 0
C. area 20 authentication message-digest
D. ip ospf message-digest-key 1 md5 CCNA

Answer: C

- area 20 authentication message-digest

Question No : 136

Which security measures can protect the control plane of a Cisco router? (Choose two.)

A. CCPr
B. Parser views
C. Access control lists
D. Port security
E. CoPP

Answer: A,E

- CCPr
- CoPP

+ control plane Policing (CoPP): you can configure this as a filter for any traffic destined to an IP address on the router itself.

+ control plane protection (CPPr): this allows for a more detailed classification of traffic (more than CoPP)

Question No : 137
In the router ospf 200, what does the value 200 stand for?

A. process ID
B. area ID
C. administrative distance value
D. ABR ID

Answer: A

- Process ID

Question No : 138
Which option describes information that must be considered when you apply an access list to a physical interface?

A. Protocol used for filtering
B. Direction of the access class
C. Direction of the access group
D. Direction of the access list

Answer: C

- Direction of the access group

R(config-if)# ip access-group [Acl No.] IN/out

Question No : 139
What is a possible reason for the error message?Router(config)#aaa server?% Unrecognized command

A. The command syntax requires a space after the word "server"
B. The command is invalid on the target device
C. The router is already running the latest operating system
D. The router is a new device on which the aaa new-model command must be applied before continuing

Answer: D

يجب ان تكتب امر aaa new-model قبل كتابة امر الخطأ

- the router is a new device on which the aaa new-model command must be applied before continuing

Question No : 140
What is the actual IOS privilege level of User Exec mode?

A. 1
B. 0
C. 5
D. 15

Answer: A

تست
A

By default, the Cisco software command-line Interface (CLI) has two levels of access commands

- user EXEC mode (Level 1)
- privilege EXEC mode (Level 15)

Question No : 141

With Cisco IOS zone-based policy firewall, by default, which three types of traffic are permitted by the router when some of the router interfaces are assigned to a zone? (Choose three.)

A. traffic flowing between a zone member interface and any interface that is not a zone member
B. traffic flowing to and from the router interfaces (the self zone)
C. traffic flowing among the interfaces that are members of the same zone
D. traffic flowing among the interfaces that are not assigned to any zone
E. traffic flowing between a zone member interface and another interface that belongs in a different zone
F. traffic flowing to the zone member interface that is returned traffic

Answer: B,C,D

- traffic flowing to and from the router interfaces (the self zone).
- traffic flowing among the interfaces that are members of the same zon
- traffic flowing among the interfaces that are not assigned by any zone.

Question No : 142

Which of the following pairs of statements is true in terms of configuring MD authentication?

A. Interface statements (OSPF, EIGRP) must be configured; use of key chain in OSPF
B. Router process (OSPF, EIGRP) must be configured; key chain in EIGRP
C. Router process (only for OSPF) must be configured; key chain in EIGRP
D. Router process (only for OSPF) must be configured; key chain in OSPF
E. Router process or interface statement for ospf must be configured; key chain in EIGRP

Answer: C E

- Router process (only for OSPF) must be configured; key chain in EIGRP
- Router process or interface statement for ospf must be configured; key chain in EIGRP

full

CE, (Choose two)

نفس سؤال سابق

Question No : 143
What encryption technology has broadest platform support

A. hardware
B. middleware
C. Software
D. File level

Answer: C

- Software

Question No : 144
What is the Cisco preferred countermeasure to mitigate CAM overflows?

A. Port security
B. Dynamic port security
C. IP source guard
D. Root guard

Answer: B

tut
B
B

كما نعلم ان ال CAM overflows هو ان يقوم ال attacker بإرسال العديد
من ال packets وكل attack packet ل source mac add. مختلف لذلك
سوف يمتلئ ال mac address table .
لمعالجة هذا النوع من ال attack يتم بواسطة Dynamic port security

Question No : 145
Which statement about communication over failover interfaces is true?

A. All information that is sent over the failover and stateful failover interfaces is sent as clear text by default.
B. All information that is sent over the failover interface is sent as clear text, but the stateful failover link is encrypted by default.
C. All information that is sent over the failover and stateful failover interfaces is encrypted by default.
D. User names, passwords, and preshared keys are encrypted by default when they are sent over the failover and stateful failover interfaces, but other information is sent as clear text.

Answer: A

- All information that is sent over the failover and stateful failover interfaces is sent as clear text by default

Question No : 146
Which option is a weakness in an information system that an attacker might leverage to gain unauthorized access to the system or its data?

A. hack
B. mitigation
C. risk
D. vulnerability
E. exploit

Answer: D

- Vulnerability

ان ال attacker ممكن ان يستخدم الثغرة في ال System اللي يكسب دخول غير مشروع له في ال System

Question No : 147
What is the effect of the ASA command crypto isakmp nat-traversal?

A. It opens port 4500 only on the outside interface.
B. It opens port 500 only on the inside interface.
C. It opens port 500 only on the outside interface.
D. It opens port 4500 on all interfaces that are IPSec enabled.

Answer: D

- It opens port 4500 on all interfaces that are IPsec enable

tut
D
D

Question No : 148
The first layer of defense which provides real-time preventive solutions against malicious traffic is provided by?

A. Banyan Filters
B. Explicit Filters
C. Outbreak Filters

Answer: C

- Outbreak Filters

Question No : 149
What is the only permitted operation for processing multicast traffic on zone-based firewalls?

A. Only control plane policing can protect the control plane against multicast traffic.
B. Stateful inspection of multicast traffic is supported only for the self-zone.
C. Stateful inspection for multicast traffic is supported only between the self-zone and the internal zone.
D. Stateful inspection of multicast traffic is supported only for the internal zone.

Answer: A

- only contral plane Policing can protect the control plane against multicast traffic

Question No : 150
What is true about the Cisco IOS Resilient Configuration feature?

A. The feature can be disabled through a remote session
B. There is additional space required to secure the primary Cisco IOS Image file
C. The feature automatically detects image and configuration version mismatch
D. Remote storage is used for securing files

Answer: C

- the feature automatically detects image and configuration version mismatch

fact
C ← cisco

Q) Which two statements about self-zone on cisco Based Firewall are true (choose two)

A - more than one interface can be assigned to the same zone

B - only one interface can be in a given zone

C - An interface can only be in one zone

D - An interface can be a number of multiple zones

E - Every device interface must be a number of a zone

Answer A C

tut

A C

- more than one interface can be assigned to the same zone
- An interface con only be in one zone

Question No : 151
Which two statements about the self zone on a Cisco zone-based policy firewall are true? (Choose Two)

A. Multiple interfaces can be assigned to the self zone.
B. Traffic entering the self zone must match a rule.
C. Zone pairs that include the self zone apply to traffic transiting the device.
D. It can be either the source zone or the destination zone.
E. It supports stateful inspection for multicast traffic.

Answer: D,E

Answer AD
- It can be either the source zone or the destination zone.
- ~~It supports stateful inspection for multicast traffic~~
- multiple interfaces can be assigned to the self zone

tut

AD
AD
AD

Question No : 152
Which technology can be used to rate data fidelity and to provide an authenticated hash for data?

A. file reputation
B. file analysis
C. signature updates
D. network blocking

Answer: A

- file reputation

tut

A → [illegible]
A

Question No : 153
What type of packet creates and performs network operations on a network device?

A. control plane packets
B. data plane packets
C. management plane packets
D. services plane packets

Answer: A

- control plane packets

انا ال control plane packets : هي ال packets الخاصه ببروتوكولات ال Routing
اي update packets وغيرها

Question No : 154
When is the best time to perform an anti-virus signature update?

A. Every time a new update is available.
B. When the local scanner has detected a new virus.
C. When a new virus is discovered in the wild.
D. When the system detects a browser hook.

Answer: A

- Every time a new update is available

Question No : 155
What command can you use to verify the binding table status?

A. show ip dhcp snooping database
B. show ip dhcp snooping binding
C. show ip dhcp snooping statistics
D. show ip dhcp pool
E. show ip dhcp source binding
F. show ip dhcp snooping

Answer: A

Show ip dhcp snooping database

tut
A

Question No : 156
What security feature allows a private IP address to access the Internet by translating it to a public address?

A. NAT
B. hairpinning
C. Trusted Network Detection
D. Certification Authority

Answer: A

Question No : 157
Which command will configure a Cisco ASA firewall to authenticate users when they enter the enable syntax using the local database with no fallback method?

A. aaa authentication enable console LOCAL SERVER_GROUP
B. aaa authentication enable console SERVER_GROUP LOCAL
C. aaa authentication enable console local
D. aaa authentication enable console LOCAL

Answer: D

الامر لكي يتم عمل authentication لل users من خلال ال local database
وبدون اي قاعدة بيانات اخرى في حالة الفشل

aaa authentication enable console LOCAL

انتبه ان ال LOCAL مكتوبة ب الكابيتل لتر

Question No : 158
You are the security administrator for a large enterprise network with many remote locations. You have been given the assignment to deploy a Cisco IPS solution.
Where in the network would be the best place to deploy Cisco IOS IPS?

A. Inside the firewall of the corporate headquarters Internet connection
B. At the entry point into the data center
C. Outside the firewall of the corporate headquarters Internet connection
D. At remote branch offices

Answer: D

- At remote branch offices

كما نعلم اننا نضع ال IPs بعد ال firewall لان ال IPs يعمل deep inspection
اكثر من ال firewall لذلك ممكن ان يتسبب ببطء الشبكة . لذلك فانا احسن
مكان لوضع ال IPs في ال remote branch office

Question No : 159
The stealing of confidential information of a company comes under the scope of:

A. Reconnaissance
B. Spoofing attack
C. Social Engineering
D. Denial of Service

Answer: C

- Social Engineering

كما نعلم ان الـ Social Engineering attack هو انتحال شخص بشركة معينة و
نه عن اصدر الشركات لوضع حلول لمشاكل الشبكة. لذلك سوف يأخذ
معلومات عن الشبكة في الشركة المستهدفة. ويتم استخدام هذه المعلومات
في نوع attack اخر

لنفس معلومات سؤال 104

Question No : 160
What are two uses of SIEM software? (Choose two.)

A. collecting and archiving syslog data
B. alerting administrators to security events in real time
C. performing automatic network audits
D. configuring firewall and IDS devices
E. scanning email for suspicious attachments

Answer: A,B

تم
AB

- collecting and archiving syslog data
- alerting adminstrator to security events in real time

Question 104
which two functions can SIEM provide? (choose two)
A correlation between logs and events from multiple systems
B - Proactive malware anlysis to block

Question No : 161
What do you use when you have a network object or group and want to use an IP address?

A. Static NAT
B. Dynamic NAT
C. identity NAT
D. Static PAT

Answer: B

- Dynamic NAT

نفس سؤال اللي فات

Question No : 162
Which 2 NAT type allows only objects or groups to reference an IP address?

A. dynamic NAT
B. dynamic PAT
C. static NAT
D. identity NAT

Answer: A,C

- dynamic NAT
- static NAT

ملاحظة: اذا اكثر من واحد في ال NAT فنستخدم ال Dynamic NAT
او اختيار واحد فقط (اول)

Question No : 163
Which type of address translation should be used when a Cisco ASA is in transparent mode?

A. Static NAT
B. Dynamic NAT
C. Overload
D. Dynamic PAT

Answer: A

عندما يكون الـ ASA بالـ transparent mode فإنه لا يدعم الـ IP address translation

لذلك يجب أن نستخدم الـ Static NAT

Question No : 164
Which protocol provides security to Secure Copy?

A. IPsec
B. SSH
C. HTTPS
D. ESP

Answer: B

- SSH

The SCP is a network protocol, which supports file transfers between hosts on a network. SCP uses Secure Shell (SSH) for data transfer and uses same mechanism for authentication.

Question No : 164
Which protocol provides security to Secure Copy?

E. IPsec
F. SSH
G. HTTPS
H. ESP

Answer: B

Question No : 165
What is the FirePOWER impact flag used for?
A. A value that indicates the potential severity of an attack.
B. A value that the administrator assigns to each signature.
C. A value that sets the priority of a signature.
D. A value that measures the application awareness.

Answer: A

attack ال يمثل impact flag ال

- A value that indicates the potential severity of an attac

Question No : 166

Which Source fire event action should you choose if you want to block only malicious traffic from a particular end user?

A. Allow with inspection
B. Allow without inspection
C. Block
D. Trust
E. Monitor

Answer: A

- Allow with inspection

Question No : 167

Which network device does NTP authenticate?

A. Only the time source
B. Only the client device
C. The firewall and the client device
D. The client device and the time source

Answer: A

- only the time source

في ال NTP فان ال NTP server يعمل authentication لل source time فقط
مو الجهاز

نفس سؤال سابق

Question No : 168
Which type of encryption technology has the broadcast platform support?

A. Middleware
B. Hardware
C. Software
D. File-level

Answer: C

- Software

Question No : 169
Refer to the exhibit.

```
209.114.111.1 configured, ipv4, sane, valid, stratum 2
ref ID 132.163.4.103  , time D7AD124D.9D6FC576 (03:17:33.614 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 46.34 msec, root disp 23.52, reach 1, sync dist 268.59
delay 63.27 msec, offset 7.9817 msec, dispersion 187.56, jitter 2.07 msec
precision 2**23, version 4

204.2.134.164 configured, ipv4, sane, valid, stratum 2
ref ID 241.199.164.101, time D7AD1419.9EB5272B (03:25:13.619 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 256
root delay 30.83 msec, root disp 4.88, reach 1, sync dist 223.80
delay 28.69 msec, offset 6.4331 msec, dispersion 187.55, jitter 1.39 msec
precision 2**20, version 4

192.168.10.7 configured, ipv4, our_master, sane, valid, stratum 3
ref ID 108.61.73.243  , time D7AD0D8F.AE79A23A (02:57:19.681 UTC Sun Aug 31 2014)
our mode client, peer mode server, our poll intvl 64, peer poll intvl 64
root delay 86.45 msec, root disp 87.82, reach 377, sync dist 134.25
delay 0.89 msec, offset 19.5087 msec, dispersion 1.69, jitter 0.84 msec
precision 2**32, version 4
```

With which NTP server has the router synchronized?

A. 192.168.10.7
B. 108.61.73.243
C. 209.114.111.1
D. 132.163.4.103
E. 204.2.134.164
F. 241.199.164.101

Answer: A

نلاحظ انه في output من الامر show ntp accociation detail

- configured :- this NTP clock source has been configured to be a server

- our master :- this local client is Synchronized to this peer

192.168.10.7 ← Ipaddress الـ NTP server الذي يعمل له الراوتر متصل به

Question No : 170
which term best describes the concept of preventing the modification of data in transit and in storage?

A. Confidentiality
B. Integrity
C. Availability
D. fidelity

Answer: B

- Integrity

كما نعلم ان Integrity تعني ان البيانات تصل الى المستلم بدون اي تغيير . اي لم يتم عمل تعديلات على البيانات عند ارسالها خلال الانتقال او الشبكة بصورة عامة

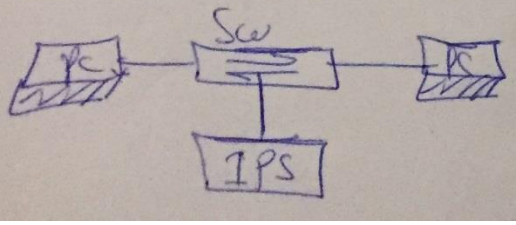
Question No : 171
Which actions can a promiscuous IPS take to mitigate an attack? (Choose three.)

A. Modifying packets
B. Requesting connection blocking
C. Denying packets
D. Resetting the TCP connection
E. Requesting host blocking
F. Denying frames

Answer: B,D,E

tut
B, D, E

- Requesting connection blocking
- Resetting the TCP connection
- Requesting host blocking



← الشكل الخاص بـ IPS promiscuous mode

2 نفس السؤال

Question No : 172

dst	src	state	conn-id	slot
10.10.10.2	10.1.1.5	QM_IDLE	1	0

While troubleshooting site-to-site VPN, you issued the show crypto isakmp sa command. What does the given output show?

A. IPSec Phase 1 is established between 10.10.10.2 and 10.1.1.5.
B. IPSec Phase 2 is established between 10.10.10.2 and 10.1.1.5.
C. IPSec Phase 1 is down due to a QM_IDLE state.
D. IPSec Phase 2 is down due to a QM_IDLE state.

Answer: A

Question No : 174
For what reason would you configure multiple security contexts on the ASA firewall?

A. To separate different departments and business units.
B. To enable the use of VRFs on routers that are adjacently connected.
C. To provide redundancy and high availability within the organization.
D. To enable the use of multicast routing and QoS through the firewall.

Answer: A

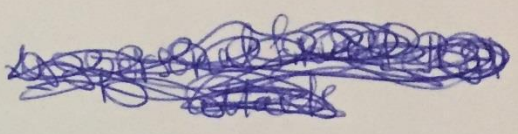
- To seperate different departments and business units.

نفس موضوع السؤال السابق

Question No : 175
Which statement about personal firewalls is true?

A. They can protect a system by denying probing requests.
B. They are resilient against kernel attacks.
C. They can protect email messages and private documents in a similar way to a VPN.
D. They can protect the network against attacks.

Answer: A



probing requests attacks يمنع النظام personal firewall ان ال

Question 109

what is a reason for an organization to deploy a personal firewall

- to protect endpoints such as desktop from malicious activity

Question No : 176
Which command do you enter to enable authentication for OSPF on an interface?

A. router(config-if)#ip ospf message-digest-key 1 md5 CISCOPASS
B. router(config-router)#area 0 authentication message-digest
C. router(config-router)#ip ospf authentication-key CISCOPASS
D. router(config-if)#ip ospf authentication message-digest

Answer: D

router(conf-if)#IP ospf authentication message-digest

tut

D

Question No : 177
Which two actions can a zone-based firewall take when looking at traffic? (Choose two)

A. Filter
B. Forward
C. Drop
D. Broadcast
E. Inspect

Answer: C,E

- Drop
- Inspect

tut

C E ← C
C E

Question No : 178
Refer to the below.

```
Router# debug tacacs

14:00:09: TAC+: Opening TCP/IP connection to 192.168.60.15 using source
10.116.0.79
14:00:09: TAC+: Sending TCP/IP packet number 383258052-1 to 192.168.60.15
(AUTHEN/START)
14:00:09: TAC+: Receiving TCP/IP packet number 383258052-2 from 192.168.60.15
14:00:09: TAC+ (383258052): received authen response status = GETUSER
14:00:10: TAC+: send AUTHEN/CONT packet
14:00:10: TAC+: Sending TCP/IP packet number 383258052-3 to 192.168.60.15
(AUTHEN/CONT)
14:00:10: TAC+: Receiving TCP/IP packet number 383258052-4 from 192.168.60.15
14:00:10: TAC+ (383258052): received authen response status = GETPASS
14:00:14: TAC+: send AUTHEN/CONT packet
14:00:14: TAC+: Sending TCP/IP packet number 383258052-5 to 192.168.60.15
(AUTHEN/CONT)
14:00:14: TAC+: Receiving TCP/IP packet number 383258052-6 from 192.168.60.15
14:00:14: TAC+ (383258052): received authen response status = PASS
14:00:14: TAC+: Closing TCP/IP connection to 192.168.60.15
```

Which statement about this debug output is true?

A. The requesting authentication request came from username GETUSER.
B. The TACACS+ authentication request came from a valid user.
C. The TACACS+ authentication request passed, but for some reason the user's connection was closed immediately.
D. The initiating connection request was being spoofed by a different source address.

Answer: B

PASS = received authen response status إذا ظهرت

- the TACACS+ authentication request came from a valid use

Question No : 179
When an IPS detects an attack, which action can the IPS take to prevent the attack from spreading?

A. Deny the connection inline.
B. Perform a Layer 6 reset.
C. Deploy an antimalware system.
D. Enable bypass mode.

Answer: A

Deny connection inline :- this action terminates the packet that triggered the action and future packets that are part of the same TCP connection.

Question No : 180
Which command is needed to enable SSH support on a Cisco Router?

A. crypto key lock rsa
B. crypto key generate rsa
C. crypto key zeroize rsa
D. crypto key unlock rsa

Answer: B

- crypto key generate rsa

Question No : 181
Which Cisco feature can help mitigate spoofing attacks by verifying symmetry of the traffic path?

A. Unidirectional Link Detection
B. Unicast Reverse Path Forwarding
C. TrustSec
D. IP Source Guard

Answer: B

- Unicast Reverse Path Forwarding (uRPF)

Question No : 182
What does the command crypto isakmp nat-traversal do?

A. Enables udp port 4500 on all IPsec enabled interfaces
B. rebooting the ASA the global **command**

fut
A

Answer: A

- Enables UDP port 4500 on all IPsec enabled interfa

Question 147
What is the effect of ASA command crypto isakmp nat-tr

A It opens port 4500 on all interfaces that are Ipsec enable

fut
A

Question No : 183
How does a device on a network using ISE receive its digital certificate during the new- device registration process?

A. ISE acts as a SCEP proxy to enable the device to receive a certificate from a central CA server.
B. ISE issues a certificate from its internal CA server.
C. ISE issues a pre-defined certificate from a local database.
D. The device requests a new certificate directly from a central CA.

Answer: A

- ISE acts as SCEP proxy to enable the device to receive a certificate from a central CA server.

106 نفس سؤال

Question No : 184
Which three statements about host-based IPS are true? (Choose three.)
A. It can view encrypted files.
B. It can have more restrictive policies than network-based IPS.
C. It can generate alerts based on behaviour at the desktop level.
D. It can be deployed at the perimeter.
E. It uses signature-based policies.
F. It works with deployed firewalls.

Answer: A,B,C

Question No : 185
What are the primary attack methods of VLAN hopping? (Choose two.)

A. VoIP hopping
B. Switch spoofing
C. CAM-table overflow
D. Double tagging

Answer: B,D

ان ال VLAN hopping هو طريقة attack يمكن من خلالها ال attacker بالوصول
الى host في vlan معينة من المفترض ان جهاز ال attacker pc في vlan
اخرى وليس من المسموح لها بالوصول الى جهاز ال host ويتم بواسطة احدى الطرق
- Switch spoofing
- Double tagging

Question No : 186
Refer to the exhibit.

```
R1> show clock detail
.22:22:35.123 UTC Tue Feb 26 2013
Time source is NTP
```

Which statement about the device time is true?
A. The time is authoritative, but the NTP process has lost contact with its servers.
B. The time is authoritative because the clock is in sync.
C. The clock is out of sync.
D. NTP is configured incorrectly.
E. The time is not authoritative.

Answer: A

من ال (.) في بداية الساعة نعرف ان
_the time is authoritative, but the NTP Process has Lost contact with its servers.