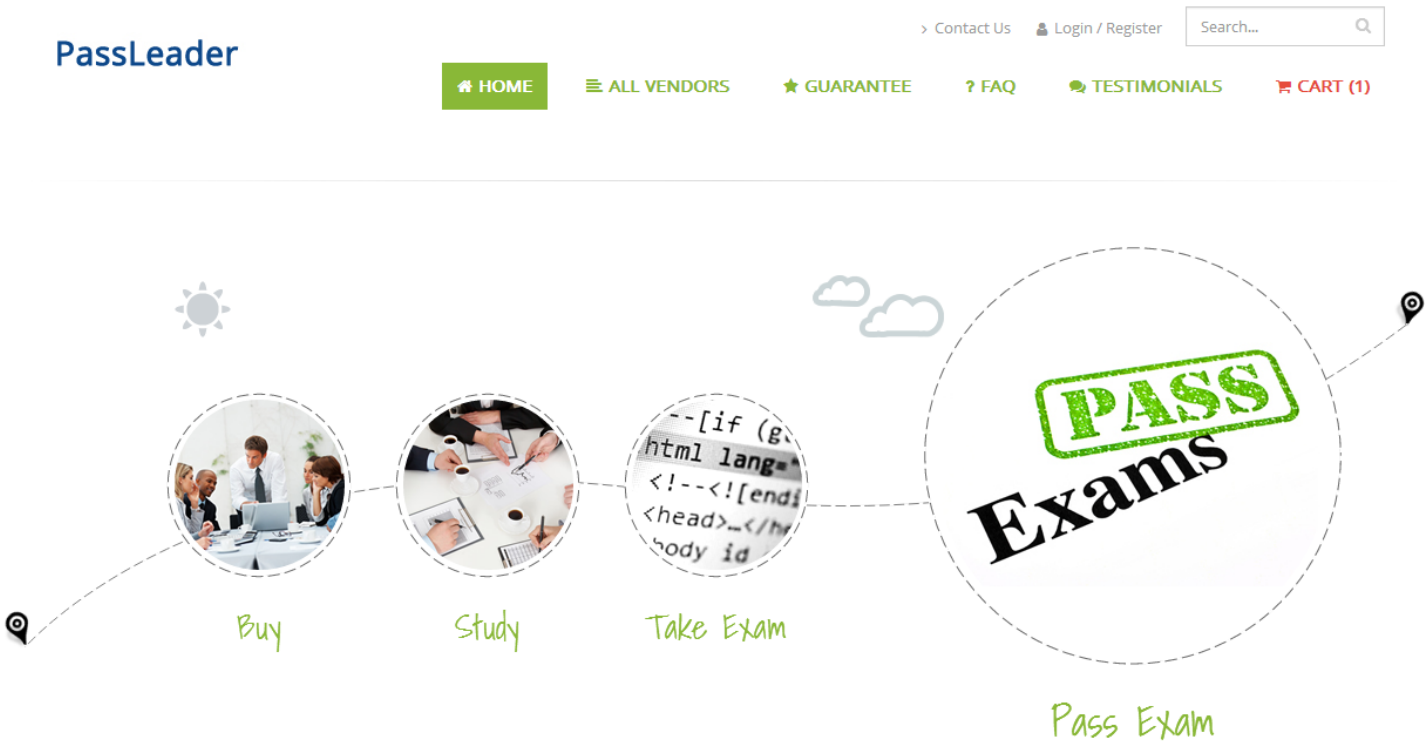
PassLeader



Try **PDF Demo** before you buy

We're not the only ones **happy** about PassLeader Practice Material ...

63159+ customers in 100+ countries use PassLeader Test Engine. Meet our customers.

VOREED GetCustom JET ORANGE iCompany Paradoxx iMessenger

http://www.passleader.top/

Latest Exam Guide & Learning Materials

Exam : **210-260**

Title : Implementing Cisco Network Security

Vendor : Cisco

Version : DEMO

NO.1 You are configuring a site-to-site tunnel between two Cisco routers by using IPsec. Which option do you set to specify the peer to which you want to connect?
A. IP address of a tunnel destination
B. IP address as part of the ISAKMP configuration
C. Tunnel group that has a peer IP address
D. IP address by using a crypto map
Answer: B

NO.2 Which option is the most effective placement of an IPS device within the infrastructure?
A. Inline, before the internet router and firewall
B. Promiscuously, before the Internet router and the firewall
C. Inline, behind the internet router and firewall
D. Promiscuously, after the Internet router and before the firewall
Answer: C
Explanation
Firewalls are generally designed to be on the network perimeter and can handle dropping a lot of the non- legitimate traffic (attacks, scans etc.) very quickly at the ingress interface, often in hardware. An IDS/IPS is, generally speaking, doing more deep packet inspections and that is a much more computationally expensive undertaking. For that reason, we prefer to filter what gets to it with the firewall line of defense before engaging the IDS/IPS to analyze the traffic flow.
Source: https://supportforums.cisco.com/discussion/12428821/correct-placement-idsips-network-architecture

NO.3 Which two resources are needed when implementing IPsec site-to-site VPN using Cisco IOS devices? (Choose two.)
A. TACSAS+
B. NTP
C. RADIUS
D. Cisco AnyConnect
E. CA
Answer: C,E

NO.4 Which quantifiable item should you consider when your organization adopts new technologies?
A. risk
B. exploits
C. vulnerability
D. threats
Answer: C

NO.5 Referencing the CIA model, in which scenario is a hash-only function most appropriate?
A. securing real-time traffic
B. securing wireless transmissions.

C. securing data at rest
D. securing data in files.
Answer: B

NO.6 Which firepower preprocessor block traffic based on IP?
A. Reputation-Based
B. Signature-Based
C. Anomaly-Based
D. Policy-Based
Answer: A
Explanation
Access control rules within access control policies exert granular control over network traffic logging and handling. Reputation-based conditions in access control rules allow you to manage which traffic can traverse your network, by contextualizing your network traffic and limiting it where appropriate.
Access control rules govern the following types of reputation-based control:
+ Application conditions allow you to perform application control, which controls application traffic based on not only individual applications, but also applications' basic characteristics: type, risk, business relevance, categories, and tags.
+ URL conditions allow you to perform URL filtering, which controls web traffic based on individual websites, as well as websites' system-assigned category and reputation.
The ASA FirePOWER module can perform other types of reputation-based control, but you do not configure these using access control rules. For more information, see:
+ Blacklisting Using Security Intelligence IP Address Reputation explains how to limit traffic based on the reputation of a connection's origin or destination as a first line of defense.
+ Tuning Intrusion Prevention Performance explains how to detect, track, store, analyze, and block the transmission of malware and other types of prohibited files.
Source:
http://www.cisco.com/c/en/us/td/docs/security/firesight/541/firepower-module-user-guide/asa-firepower- module-user-guide-v541/AC-Rules-App-URL-Reputation.html

NO.7 What is example of social engineering
A. Watching other user put in username and password (something around there)
B. Gaining access to a building through an unlocked door.
C. something about inserting a random flash drive.
D. gaining access to server room by posing as IT
Answer: D

NO.8 Which IPS mode is less secure than other options but allows optimal network throughput?
A. transparent mode
B. Promiscuous mode
C. inline-bypass mode
D. inline mode
Answer: B
Explanation

The recommended IPS deployment mode depends on the goals and policies of the enterprise. IPS inline mode is more secure because of its ability to stop malicious traffic in real-time, however it may impact traffic throughput if not properly designed or sized. Conversely, IPS promiscuous mode has less impact on traffic throughput but is less secure because there may be a delay in reacting to the malicious traffic.
https://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/SAFE_RG/safesmallentnetworks.html

NO.9 Refer to the exhibit.

```
UDP outside  209.165.201.225:53 inside  10.0.0.10:52464, idle 0:00:01, bytes 266, flags -
```

What type of firewall would use the given configuration line?

A. a personal firewall
B. a stateful firewall
C. a stateless firewall
D. a proxy firewall
E. an application firewall

Answer: B

Explanation
The output is from "show conn" command on an ASA. This is another example output I've simulated
ciscoasa# show conn
20 in use, 21 most used
UDP OUTSIDE 172.16.0.100:53 INSIDE 10.10.10.2:59655, idle 0:00:06, bytes 39, flags -

NO.10 Which two SNMPv3 services support its capabilities as a secure network management protocol?

A. accounting
B. authentication
C. the shared secret key
D. access control
E. authorization

Answer: B,D

NO.11 The stealing of confidential information of a company comes under the scope of

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

Answer: D

NO.12 Where is file reputation performed in a Cisco AMP solution?

A. in the cloud
B. on a Cisco ESA
C. on an endpoint

D. on a perimeter firewall
Answer: C

NO.13 Which two characteristics of the TACACS+ protocol are true? (Choose two.)
A. encrypts the body of every packet
B. is an open RFC standard protocol
C. separates AAA functions
D. uses UDP ports 1645 or 1812
E. offers extensive accounting capabilities
Answer: A,C
Explanation
http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml Packet Encryption RADIUS encrypts only the password in the access-request packet, from the client to the server. The remainder of the packet is unencrypted. Other information, such as username, authorized services, and accounting, can be captured by a third party.
TACACS+ encrypts the entire body of the packet but leaves a standard TACACS+ header. Within the header is a field that indicates whether the body is encrypted or not. For debugging purposes, it is useful to have the body of the packets unencrypted. However, during normal operation, the body of the packet is fully encrypted for more secure communications.
Authentication and Authorization RADIUS combines authentication and authorization. The access-accept packets sent by the RADIUS server to the client contain authorization information. This makes it difficult to decouple authentication and authorization.
TACACS+ uses the AAA architecture, which separates AAA. This allows separate authentication solutions that can still use TACACS+ for authorization and accounting. For example, with TACACS+, it is possible to use Kerberos authentication and TACACS+ authorization and accounting. After a NAS authenticates on a Kerberos server, it requests authorization information from a TACACS+ server without having to re-authenticate. The NAS informs the TACACS+ server that it has successfully authenticated on a Kerberos server, and the server then provides authorization information.
During a session, if additional authorization checking is needed, the access server checks with a TACACS+ server to determine if the user is granted permission to use a particular command. This provides greater control over the commands that can be executed on the access server while decoupling from the authentication mechanism.

NO.14 Refer to the exhibit.

```
R1#show snmp
Chassis: FTX123456789
0 SNMP packets input
    6 Bad SNMP version errors
    3 Unknown community name
    9 Illegal operation for community name supplied
    4 Encoding errors
    2 Number of requested variables
    0 Number of altered variables
    98 Get-request PDUs
    12 Get-next PDUs
    2 Set-request PDUs
    0 Input queue packet drops (Maximum queue size 1000)
0 SNMP packets output
    0 Too big errors (Maximum packet size 1500)
    0 No such name errors
    0 Bad values errors
    0 General errors
    31 Response PDUs
    1 Trap PDUs
```

How many times was a read-only string used to attempt a write operation?

A. 6

B. 3

C. 4

D. 9

E. 2

Answer: D

Explanation

To check the status of Simple Network Management Protocol (SNMP) communications, use the show snmp command in user EXEC or privileged EXEC mode.

Illegal operation for community name supplied: Number of packets requesting an operation not allowed for that community Source:

http://www.cisco.com/c/en/us/td/docs/ios/netmgmt/command

NO.15 Which two statements about the self zone on Cisco zone based policy firewall are true ? (Choose two)

A. it can be either the source zone or destination zone .

B. zone pairs that include the self zone apply to traffic transiting the device.

C. it supports statefull inspection for multicast traffic

D. multiple interfaces can be assigned to the self zone .

E. traffic entering the self zone must match a rule.

Answer: A,D

NO.16 What is the purpose of a honeypot IPS?
A. To collect information about attacks
B. To normalize streams
C. To create customized policies
D. To detect unknown attacks
Answer: A
Explanation
Honeypot systems use a dummy server to attract attacks. The purpose of the honeypot approach is to distract attacks away from real network devices. By staging different types of vulnerabilities in the honeypot server, you can analyze incoming types of attacks and malicious traffic patterns.
Source:
http://www.ciscopress.com/articles/article.asp?p=1336425

NO.17 Which TACACS+ server-authentication protocols are supported on Cisco ASA firewalls? (Choose three.)
A. PEAP
B. MS-CHAPv2
C. EAP
D. PAP
E. MS-CHAPv1
F. ASCII
Answer: D,E,F
Explanation
The ASA supports TACACS+ server authentication with the following protocols: ASCII, PAP, CHAP, and MS- CHAPv1.
Source:
http://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/general/asa_91_general_config/ aaa_tacacs.pdf

NO.18 How can you stop reconnaissance attack with cdp.
A. disable CDP on ports connected to end points (or Disable CPD on edfe ports)
B. enable dynamic ARP inspection on all untrusted ports
C. disable CDP on trunk ports
D. enable dot1x on all ports that are connected to other switches
Answer: A

NO.19 In which two models can the Cisco Web Security Appliance be deployed? (Choose two.)
A. explicit proxy mode
B. as a transparent proxy using the HyperText Transfer Protocol
C. explicit active mode
D. as a transparent proxy using the Secure Sockets Layer protocol
E. as a transparent proxy using the Web Cache Communication Protocol
Answer: A,E

Reference:
https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-smart-businessarchitecture/sba_w

NO.20 Which feature can help a router or switch maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch?
A. Cisco Express Forwarding
B. Service Policy
C. Control Plane Policing
D. Policy Map
Answer: C

NO.21 How can you allow bidirational traffic?
A. dynamic NAT
B. static NAT
C. multi-NAT
D. dynamic PAT
Answer: B
Explanation
Bidirectional initiation--Static NAT allows connections to be initiated bidirectionally, meaning both to the host and from the host.
Source: http://www.cisco.com/c/en/us/td/docs/securi
ty/asa/asa83/configuration/guide/config/nat_overview.html

NO.22 Which statement about NAT table evaluation in the ASA is true?
A. Auto NAT policies are applied first
B. Manual NAT policies are applied first
C. The ASA uses the most specific match
D. After-auto NAT polices are applied first
Answer: B

NO.23 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
Explanation
You can configure AnyConnect to establish a VPN session automatically after the user logs in to a computer.
The VPN session remains open until the user logs out of the computer, or the session timer or idle session timer expires. The group policy assigned to the session specifies these timer values. If AnyConnect loses the connection with the ASA, the ASA and the client retain the resources assigned

to the session until one of these timers expire. AnyConnect continually attempts to reestablish the connection to reactivate the session if it is still open; otherwise, it continually attempts to establish a new VPN session.
Source:
http://www.cisco.com/c/en/us/td/docs/security/vpn_client/anyconnect/anyconnect30/administration/ guide/anyconnectadmin30/ac03vpn.pdf

NO.24 Which of the following pairs of statements is true in terms of configuring MD authentication?
A. Router process (only for OSPF) must be configured; key chain in OSPF
B. Router process (OSPF, EIGRP) must be configured; key chain in EIGRP
C. Interface statements (OSPF, EIGRP) must be configured; use of key chain in OSPF
D. Router process (only for OSPF) must be configured; key chain in EIGRP
Answer: D

NO.25 What command can you use to verify the binding table status?
A. show ip dhcp source binding
B. show ip dhcp snooping binding
C. show ip dhcp snooping statistics
D. show ip dhcp snooping
E. show ip dhcp pool
F. show ip dhcp snooping database
Answer: F
Explanation
A device's burned-in address is its MAC address. So by changing it to something else may trick hosts on the network into sending packets to it.

NO.26 What is the best way to confirm that AAA authentication is working properly?
A. Use the Cisco-recommended configuration for AAA authentication.
B. Use the test aaa command.
C. Ping the NAS to confirm connectivity.
D. Log into and out of the router, and then check the NAS authentication log.
Answer: B
Explanation
#test aaa group tacacs+ admin cisco123 legacy - A llow verification of the authentication function working between the AAA client (the router) and the ACS server (the AAA server).
Source: Cisco Official Certification Guide, Table 3-6 Command Reference, p.68

NO.27 What technology can you use to provide data confidentiality, data integrity and data origin authentication on your network?
A. IKE
B. Certificate Authority
C. Data Encryption Standards
D. IPSec
Answer: D

NO.28 Which command enables authentication at the OSPFv2 routing process level?
A. ip ospf authentication message-digest
B. area 0 authentication message-digest
C. ip ospf message-digest-key 1 md5 C1sc0!
D. area 0 authentication ipsec spi 500 md5 1 234567890ABCDEF1234567890ABCDEF
Answer: B

NO.29 What show command can see vpn tunnel establish with traffic passing through.
A. show crypto ipsec transform-set
B. show crypto ipsec sa
C. show crypto session
D. show crypto isakmp sa
Answer: B
Explanation
#show crypto ipsec sa - This command shows IPsec SAs built between peers In the output you see
#pkts encaps: 345, #pkts encrypt: 345, #pkts digest 0
#pkts decaps: 366, #pkts decrypt: 366, #pkts verify 0
which means packets are encrypted and decrypted by the IPsec peer.
Source:
http://www.cisco.com/c/en/us/support/docs/security-vpn/ipsec-negotiation-ike-protocols/5409-ipsec- debug-00.html#ipsec_sa

NO.30 On an ASA, which maps are used to identify traffic?
A. Class maps
B. Route maps
C. Policy maps
D. Service maps
Answer: A