Vendor: Palo Alto Networks

Exam Code: PCNSE

Exam Name: Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.0

Version: DEMO

QUESTION 1
The decision to upgrade to PAN-OS 10.2 has been approved. The engineer begins the process by upgrading the Panorama servers, but gets an error when trying to install.

When performing an upgrade on Panorama to PAN-OS 10.2, what is the potential cause of a failed install?

A. GlobalProtect agent version
B. Outdated plugins
C. Management only mode
D. Expired certificates

Answer: B
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/upgrade-panorama-plugins/panorama-plugins-upgrade-downgrade-considerations
Before you upgrade to PAN-OS 11.0, you must download the Panorama plugin version supported on PAN-OS 11.0 for all plugins installed on Panorama. This is required to successfully upgrade to PAN-OS 11.0. See the Compatibility Matrixfor more information.

QUESTION 2
A firewall administrator wants to have visibility on one segment of the company network. The traffic on the segment is routed on the Backbone switch. The administrator is planning to apply Security rules on segment X after getting the visibility.
There is already a PAN-OS firewall used in L3 mode as an internet gateway, and there are enough system resources to get extra traffic on the firewall. The administrator needs to complete this operation with minimum service interruptions and without making any IP changes.
What is the best option for the administrator to take?

A. Configure the TAP interface for segment X on the firewall
B. Configure a Layer 3 interface for segment X on the firewall.
C. Configure vwire interfaces for segment X on the firewall.
D. Configure a new vsys for segment X on the firewall.

Answer: C
Explanation:
As it specifically states in the question that security rules will be applied, VWire is the only method that allows this without making any IP address changes.

QUESTION 3
A network engineer is troubleshooting a VPN and wants to verify whether the decapsulation/encapsulation counters are increasing.
Which CLI command should the engineer run?

A. Show running tunnel flow lookup
B. Show vpn flow name <tunnel name>
C. Show vpn ipsec-sa tunnel <tunnel name>
D. Show vpn tunnel name | match encap

Answer: B
Explanation:
Check if encapsulation and decapsulation bytes are increasing. If the firewall is passing traffic,

then both values should be increasing.
> show vpn flow name <tunnel.id/tunnel.name> | match bytes
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClivCAC

QUESTION 4
A consultant deploys a PAN-OS 11.0 VM-Series firewall with the Web Proxy feature in Transparent Proxy mode.

Which three elements must be in place before a transparent web proxy can function? (Choose three.)

A. User-ID for the proxy zone
B. DNS Security license
C. Prisma Access explicit proxy license
D. Cortex Data Lake license
E. Authentication Policy Rule set to default-web-form

Answer: ABC
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

QUESTION 5
An organization is interested in migrating from their existing web proxy architecture to the Web Proxy feature of their PAN-OS 11.0 firewalls. Currently, HTTP and SSL requests contain the destination IP address of the web server and the client browser is redirected to the proxy.

Which PAN-OS proxy method should be configured to maintain this type of traffic flow?

A. SSL forward proxy
B. Explicit proxy
C. Transparent proxy
D. DNS proxy

Answer: C
Explanation:
For the transparent proxy method, the request contains the destination IP address of the web server and the proxy transparently intercepts the client request (either by being in-line or by traffic steering). There is no client configuration and Panorama is optional. Transparent proxy requires a loopback interface, User-ID configuration in the proxy zone, and specific Destination NAT (DNAT) rules. Transparent proxy does not support X-Authenticated Users (XAU) or Web Cache Communications Protocol (WCCP).
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

QUESTION 6
Which new PAN-OS 11.0 feature supports IPv6 traffic?

A. OSPF
B. IKEv1
C. DHCP Server

D. DHCPv6 Client with Prefix Delegation

Answer: D
Explanation:
https://docs.paloaltonetworks.com/compatibility-matrix/ipv6-support-by-feature/ipv6-support-by-feature-table

QUESTION 7
An administrator allocates bandwidth to a Prisma Access Remote Networks compute location with three remote networks.
What is the minimum amount of bandwidth the administrator could configure at the compute location?

A. 90Mbps
B. 300 Mbps
C. 75Mbps
D. 50Mbps

Answer: D
Explanation:
The number you specify for the bandwidth applies to both the egress and ingress traffic for the remote network connection. If you specify a bandwidth of 50 Mbps, Prisma Access provides you with a remote network connection with 50 Mbps of bandwidth on ingress and 50 Mbps on egress. Your bandwidth speeds can go up to 10% over the specified amount without traffic being dropped; for a 50 Mbps connection, the maximum bandwidth allocation is 55 Mbps on ingress and 55 Mbps on egress (50 Mbps plus 10% overage allocation).
https://docs.paloaltonetworks.com/prisma/prisma-access/prisma-access-panorama-admin/prisma-access-for-networks/how-to-calculate-network-bandwidth

QUESTION 8
An organization conducts research on the benefits of leveraging the Web Proxy feature of PAN-OS 11.0.

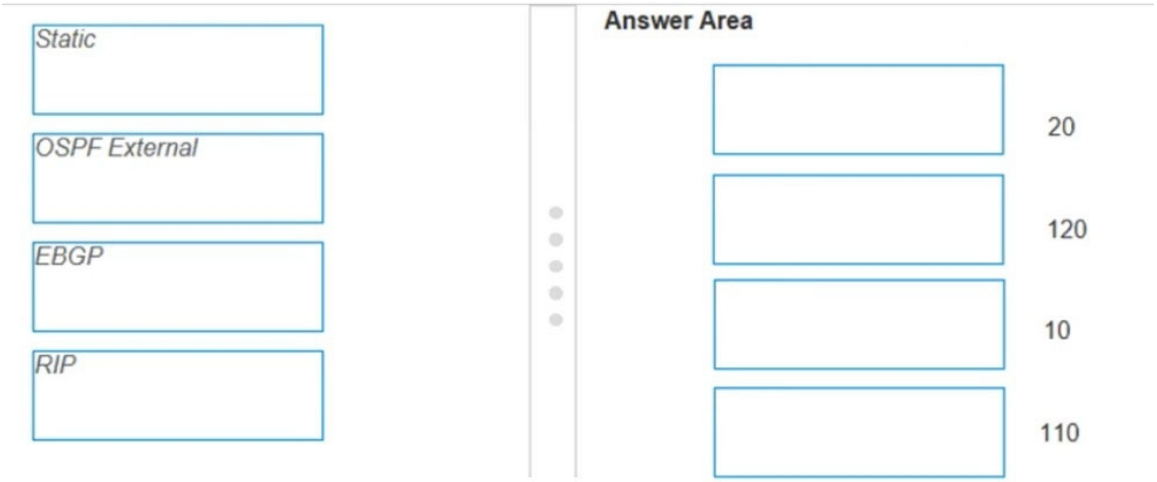
What are two benefits of using an explicit proxy method versus a transparent proxy method? (Choose two.)

A. No client configuration is required for explicit proxy, which simplifies the deployment complexity.
B. Explicit proxy supports interception of traffic using non-standard HTTPS ports.
C. It supports the X-Authenticated-User (XAU) header, which contains the authenticated username in the outgoing request.
D. Explicit proxy allows for easier troubleshooting, since the client browser is aware of the existence of the proxy.

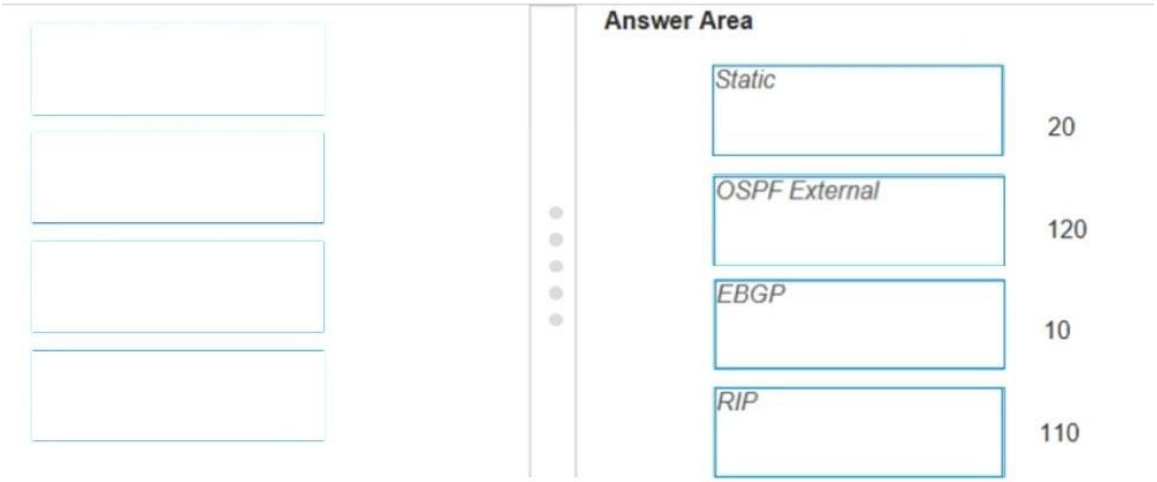
Answer: CD
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy

QUESTION 9
Drag and Drop Question

An engineer is troubleshooting traffic routing through the virtual router. The firewall uses multiple routing protocols, and the engineer is trying to determine routing priority Match the default Administrative Distances for each routing protocol.



Answer:



Explanation:
Static - Range is 10-240; default is 10.
OSPF Internal - Range is 10-240; default is 30.
OSPF External - Range is 10-240; default is 110.
IBGP - Range is 10-240; default is 200.
EBGP- Range is 10-240; default is 20.
RIP - Range is 10-240; default is 120.

QUESTION 10
An engineer wants to implement the Palo Alto Networks firewall in VWire mode on the internet gateway and wants to be sure of the functions that are supported on the vwire interface.
What are three supported functions on the VWire interface? (Choose three)

A. NAT
B. QoS
C. IPSec
D. OSPF
E. SSL Decryption

Answer: ABE
Explanation:
The virtual wire supports blocking or allowing traffic based on virtual LAN (VLAN) tags, in addition to supporting security policy rules, App-ID, Content-ID, User-ID, decryption, LLDP, active/passive and active/active HA, QoS, zone protection (with some exceptions), non-IP protocol protection, DoS protection, packet buffer protection, tunnel content inspection, and NAT.
https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-networking-admin/configure-interfaces/virtual-wire-interfaces

QUESTION 11
A consultant advises a client on designing an explicit Web Proxy deployment on PAN-OS 11.0. The client currently uses RADIUS authentication in their environment.

Which two pieces of information should the consultant provide regarding Web Proxy authentication? (Choose two.)

A. Kerberos or SAML authentication need to be configured.
B. RADIUS is only supported for a transparent Web Proxy.
C. RADIUS is not supported for explicit or transparent Web Proxy.
D. LDAP or TACACS+ authentication need to be configured.

Answer: AC
Explanation:
For the explicit proxy method, the request contains the destination IP address of the configured proxy and the client browser sends requests to the proxy directly. You can use one of following methods to authenticate users with the explicit proxy:
Kerberos, which requires a web proxy license.
SAML 2.0, which requires Panorama, a Prisma Access license, the Cloud Services 3.2.1 plugin (and later versions), and the add-on web proxy license.
Cloud Identity Engine, which requires Panorama, a Prisma Access license, the Cloud Services 3.2.1 plugin (and later versions), and the add-on web proxy license.
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-new-features/networking-features/web-proxy#id3d1ea0dd-360f-44ee-8c48-30678c80d509_id2b5c6385-2ec6-4ba8-b1f1-2bea8b5139f5

QUESTION 12
A security engineer wants to upgrade the company's deployed firewalls from PAN-OS 10.1 to 11.0.x to take advantage of the newTLSv1.3 support for management access.

What is the recommended upgrade path procedure from PAN-OS 10.1 to 11.0.x?

A. Required: Download and install the latest preferred PAN-OS 10.1 maintenance release and reboot.
Required: Download PAN-OS 10.2.0.
Optional: Install the latest preferred PAN-OS 10.2 maintenance release.
Required: Download PAN-OS 11.0.0.
Required: Download and install the desired PAN-OS 11.0.x.

B. Optional: Download and install the latest preferred PAN-OS 10.1 release.
Optional: Install the latest preferred PAN-OS 10.2 maintenance release.
Required: Download PAN-OS 11.0.0.
Required: Download and install the desired PAN-OS 11.0.x.

C. Required: Download PAN-OS 10.2.0 or earlier release that is not EOL.
Required: Download and install the latest preferred PAN-OS 10.2 maintenance release and reboot.
Required: Download PAN-OS 11.0.0.
Required: Download and install the desired PAN-OS 11.0.x.

D. Required: Download and install the latest preferred PAN-OS 10.1 maintenance release and reboot.
Required: Download PAN-OS 10.2.0.
Required: Download and install the latest preferred PAN-OS 10.2 maintenance release and reboot.
Required: Download PAN-OS 11.0.0.
Required: Download and install the desired PAN-OS 11.0.x.

Answer: B
Explanation:
https://docs.paloaltonetworks.com/pan-os/11-0/pan-os-upgrade/upgrade-pan-os/upgrade-the-firewall-pan-os/determine-the-upgrade-path

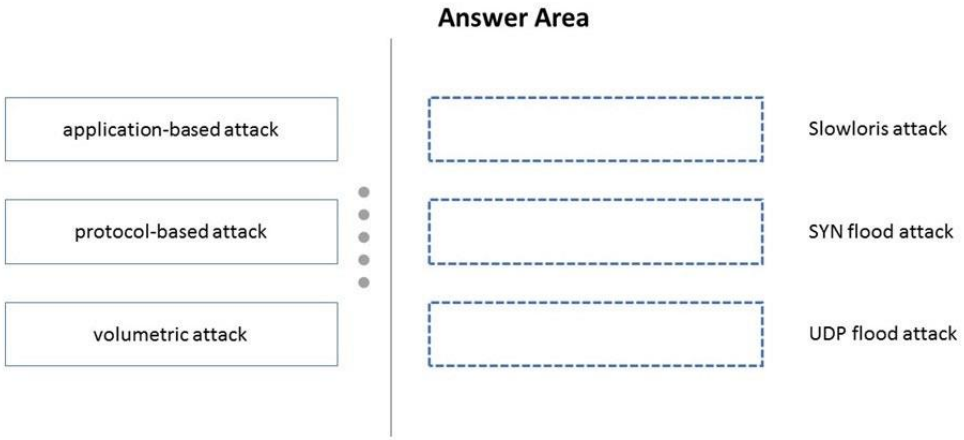
QUESTION 13
A users traffic traversing a Palo Alto networks NGFW sometimes can reach http //www company com At other times the session times out. At other times the session times out The NGFW has been configured with a PBF rule that the user traffic matches when it goes to http://www.company.com goes to http://www company com
How can the firewall be configured to automatically disable the PBF rule if the next hop goes down?

A. Create and add a monitor profile with an action of fail over in the PBF rule in question
B. Create and add a monitor profile with an action of wait recover in the PBF rule in question
C. Configure path monitoring for the next hop gateway on the default route in the virtual router
D. Enable and configure a link monitoring profile for the external interface of the firewall

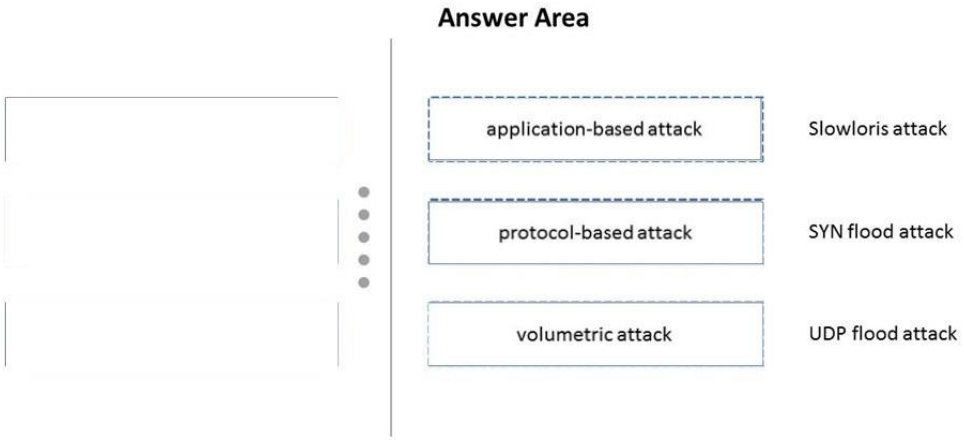
Answer: A
Explanation:
https://docs.paloaltonetworks.com/pan-os/10-2/pan-os-web-interface-help/network/network-network-profiles/network-network-profiles-monitor
A monitor profile is used to monitor IPSec tunnels and to monitor a next-hop device for policy-based forwarding (PBF) rules. In both cases, the monitor profile is used to specify an action to take when a resource (IPSec tunnel or next-hop device) becomes unavailable.
wait-recover - Wait for the tunnel to recover; do not take additional action. Packets will continue to be sent according to the PBF rule.
fail-over - Traffic will fail over to a backup path, if one is available. The firewall uses routing table lookup to determine routing for the duration of this session.

QUESTION 14
Drag and Drop Question

Based on PANW Best Practices for Planning DoS and Zone Protection, match each type of DoS attack to an example of that type of attack.



Answer:



Explanation:
Application-Based Attacks
-- Target weaknesses in a particular application and try to exhaust its resources so legitimate users can't use it. An example is the Slowloris attack.
Protocol-Based Attacks
-- Also known as state-exhaustion attacks, they target protocol weaknesses. A common example is a SYN flood attack.
Volumetric Attacks
- -High-volume attacks that attempt to overwhelm the available network resources, especially bandwidth, and bring down the target to prevent legitimate users from accessing its resources. An example is a UDP flood attack.

QUESTION 15
The manager of the network security team has asked you to help configure the company's Security Profiles according to Palo Alto Networks best practice. As part of that effort, the manager has assigned you the Vulnerability Protection profile for the internet gateway firewall.
Which action and packet-capture setting for items of high severity and critical severity best matches Palo Alto Networks best practice'?

A. action 'reset-both' and packet capture 'extended-capture'
B. action 'default' and packet capture 'single-packet'
C. action 'reset-both' and packet capture 'single-packet'
D. action 'reset-server' and packet capture 'disable'

Answer: A
Explanation:
"Enable extended-capture for critical, high, and medium severity events and single-packet capture for low severity events. "
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-web-interface-help/objects/objects-security-profiles-vulnerability-protection

QUESTION 16
An administrator is using Panorama and multiple Palo Alto Networks NGFWs. After upgrading all devices to the latest PAN-OS software, the administrator enables log forwarding from the firewalls to Panorama. Pre-existing logs from the firewalls are not appearing in PanoramA.
Which action would enable the firewalls to send their pre-existing logs to Panorama?

A. Use the import option to pull logs.
B. Export the log database
C. Use the scp logdb export command
D. Use the ACC to consolidate the logs

Answer: C
Explanation:
commands:
request logdb
migrate-to-panorama start end-timestart-timetype
https://docs.paloaltonetworks.com/panorama/9-0/panorama-admin/set-up-panorama/install-content-and-software-updates-for-panorama/migrate-panorama-logs-to-new-log-format

QUESTION 17
An engineer is creating a security policy based on Dynamic User Groups (DUG) What benefit does this provide?

A. Automatically include users as members without having to manually create and commit policy or group changes
B. DUGs are used to only allow administrators access to the management interface on the Palo Alto Networks firewall
C. It enables the functionality to decrypt traffic and scan for malicious behaviour for User-ID based policies
D. Schedule commits at a regular intervals to update the DUG with new users matching the tags specified

Answer: A
Explanation:
Dynamic user groups help you to create policy that provides auto-remediation for anomalous user behavior and malicious activity while maintaining user visibility. Previously, quarantining users in response to suspicious activity meant time-and resource-consuming updates for all members of the group or updating the IP address-to-username mapping to a label to enforce policy at the cost of user visibility, as well as having to wait until the firewall checked the traffic. Now, you can configure a dynamic user group to automatically include users as members without having to manually create and commit policy or group changes and still maintain user-to-data correlation at the device level before the firewall even scans the traffic.
https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/user-id-features/dynamic-user-groups.html

QUESTION 18
A bootstrap USB flash drive has been prepared using a Linux workstation to load the initial configuration of a Palo Alto Networks firewall. The USB flash drive was formatted using file system NTFS and the initial configuration is stored in a file named init-cfg.txt. The contents of init-cfg.txt in the USB flash drive are as follows:

```
type=static
ip-address=10.5.107.19
default-gateway=10.5.107.1
netmask=255.255.255.0
ipv6-address=2001:400:f00::1/64
ipv6-default-gateway=2001:400:f00::2
hostname=Ca-FW-DC1
panorama-server=10.5.107.20
panorama-server-2=10.5.107.21
tplname=FINANCE_TG4
dgname=finance_dg
dns_primary=10.5.6.6
dns-secondary=10.5.6.7
op-command-modes=multi-vsys, jumbo-frame
dhcp-send-hostname=no
dhcp-send-client-id=no
dhcp-accept-server-hostname=no
dhcp-accept-server-domain=no
```

The USB flash drive has been inserted in the firewalls USB port, and the firewall has been powered on. Upon boot, the firewall fails to begin the bootstrapping process. The failure is caused because:

A. the bootstrap.xml file is a required file, but it is missing
B. init-cfg.txt is an incorrect filename, the correct filename should be init-cfg.xml
C. The USB must be formatted using the ext4 file system
D. There must be commas between the parameter names and their values instead of the equal symbols
E. The USB drive has been formatted with an unsupported file system

Answer: E
Explanation:
The USB flash drive that bootstraps a hardware-based Palo Alto Networks firewall must support one of the following:
File Allocation Table 32 (FAT32)
Third Extended File System (ext3)
The firewall can bootstrap from the following flash drives with USB2.0 or USB3.0 connectivity:
https://docs.paloaltonetworks.com/pan-os/10-0/pan-os-admin/firewall-administration/bootstrap-the-firewall/usb-flash-drive-support.html#id3cfc3106-f7ab-4eee-82b7-1ca62ec5e997

QUESTION 19
An administrator deploys PA-500 NGFWs as an active/passive high availability pair. The devices are not participating in dynamic routing, and preemption is disabled.
What must be verified to upgrade the firewalls to the most recent version of PAN-OS?software?

A. Antivirus update package.
B. Applications and Threats update package.
C. User-ID agent.
D. WildFire update package.

Answer: B
Explanation:
Before you upgrade, make sure the firewall is running a version of app + threat (content version) that meets the minimum requirement of the new PAN-OS (see release notes). We recommend always running the latest version of content to ensure the most accurate and effective protections are being applied.
https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRrCAK

QUESTION 20
A firewall administrator requires an A/P HA pair to fail over more quickly due to critical business application uptime requirements.

What is the correct setting?

A. Change the HA timer profile to "user-defined" and manually set the timers.
B. Change the HA timer profile to "fast".
C. Change the HA timer profile to "aggressive" or customize the settings in advanced profile.
D. Change the HA timer profile to "quick" and customize in advanced profile.

Answer: C
Explanation:
Use the Recommended profile for typical failover timer settings and the Aggressive profile for faster failover timer settings. The Advanced profile allows you to customize the timer values to suit your network requirements.
Reference: https://docs.paloaltonetworks.com/pan-os/9-0/pan-os-admin/high-availability/set-up-activepassive-ha/configure-activepassive-ha.html

Thank You for Trying Our Product

Braindump2go Certification Exam Features:

★ More than **99,900** Satisfied Customers Worldwide.

★ Average **99.9%** Success Rate.

★ **Free Update** to match latest and real exam scenarios.

★ **Instant Download** Access! No Setup required.

★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.

★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.

★ **100%** Guaranteed Success or **100%** Money Back Guarantee.

★ **Fast**, helpful support **24x7**.

View list of all certification exams: http://www.braindump2go.com/all-products.html

10% Discount Coupon Code: **ASTR14**