PassQueen
a.k.a dumpsqueen.com

Brocade Certified vRouter Engineer

Brocade 170-010

Version Demo

Total Demo Questions: 10

Total Premium Questions: 107

Buy Premium PDF

https://passqueen.com

support@passqueen.com

QUESTION NO: 1

When configuring single-area OSPF, which area number should you use?

A. 0

B. 1

C. 2

D. 10

ANSWER: A

Explanation:

The correct area number for a standard single-area OSPF deployment is **0**. Area 0 is the OSPF backbone area and is represented internally by the Area ID 0.0.0.0. In a single-area design, placing every participating OSPF interface and router in the backbone provides the simplest topology: all routers exchange link-state information within one common area, form adjacencies with their eligible neighbors, and calculate routes from the same area link-state database.

This choice also follows the fundamental OSPF area hierarchy used when a deployment later grows beyond a single area. OSPF specifies the backbone as the central area through which inter-area routing is organized, so beginning with area 0 avoids a redesign merely to establish the backbone when additional areas are introduced. On Brocade vRouter/Vyatta-style configurations, the OSPF area is consequently commonly configured as area 0 for a basic, one-area routing domain. The OSPF version 2 specification defines the backbone and its role in the area architecture: RFC 2328, OSPF Version 2. A practical configuration reference showing OSPF area-based configuration is available in the VyOS OSPF documentation.

QUESTION NO: 2

Which three commands display whether a firewall rule has been matched by traffic? (Choose three.)

A. show firewall

B. show log

C. show firewall name statistics

D. show firewall statistics

E. show firewall log

ANSWER: A C D

Explanation:

`show firewall`, `show firewall name <name> statistics`, and `show firewall statistics` provide firewall rule match information through packet and byte counters maintained as traffic is processed. The general `show firewall` command presents the configured firewall rule sets and their rule details, including counters that indicate whether traffic has reached a rule. For focused troubleshooting of one rule set, `show firewall name <name> statistics` displays statistics for the specified firewall name, allowing an engineer to verify which individual rules are receiving packets. `show firewall statistics` supplies the broader firewall statistics view, which is useful for checking rule activity across configured firewall policies. A nonzero packet counter is direct evidence that traffic has matched the applicable rule; byte counters provide the associated traffic volume. These operational show commands are therefore appropriate when validating rule order, confirming that traffic reaches the expected policy, or troubleshooting an unexpected permit or drop. See the Brocade documentation download portal for Vyatta Network OS firewall command and configuration guides: Broadcom Technical Documentation. Brocade product documentation and legacy software resources are also available through Broadcom Support Download Search.

QUESTION NO: 3

vyatta@vyatta:~$ show interfaces

Codes: S - State, L - Link, u - Up, D - Down, A - Admin Down

Interface IP Address S/L Description

--------- ---------- --- -----------

eth0 172.24.42.52/24 u/u

eth1 192.168.12.2 /24 u/u

192.168.129.2/24

192.168.130.2/24

192.168.131.2/24

eth2 192.168.23.2/24 u/u

eth3 192.168.128.2/24 u/u

eth3.10 192.168.132.2/24

eth3.20 192.168.133.2/24

vyatta@vyatta:~$

Which interface has VLANs associated with it?

A. eth0

B. eth1

C. eth2

D. eth3

ANSWER: D

Explanation:

eth3 is the interface with VLANs associated with it. The interface listing includes the logical interfaces `eth3.10` and `eth3.20`. In Vyatta/VyOS-style interface naming, a period followed by a numeric identifier denotes a VLAN subinterface: the portion before the period identifies the physical parent interface, and the number after it is the IEEE 802.1Q VLAN ID. Therefore, `eth3.10` is the VLAN 10 subinterface on physical interface `eth3`, and `eth3.20` is the VLAN 20 subinterface on that same physical interface. Each subinterface can have its own Layer 3 address, as shown by the distinct addresses assigned to these entries, while traffic is carried through the shared parent Ethernet interface with VLAN tagging. This differs from merely having multiple IP addresses configured directly on one interface: the explicit dotted subinterface names provide the evidence of VLAN configuration. The relevant Ethernet VLAN encapsulation is defined by IEEE 802.1Q; see the IEEE 802.1Q overview. VyOS configuration documentation also describes VLAN interfaces as a parent interface combined with a VLAN identifier: VyOS Ethernet interface documentation.

QUESTION NO: 4

vyatta@vyatta:~$ show system login users

Username Type Tty From Last login

operator vyatta hvc0 Mon Jun 17 18:34:25 2013

vyatta vyatta pts/0 10.224.7.101 Wed Jun 19 20:47:39 2013

vyatta@vyatta:~$

Based on the output, which statement is true?

A. User operator last connected through the device console.

B. User vyatta is currently logged in to the system.

C. User vyatta last connected using SSH.

D. User operator has read-only privileges.

ANSWER: B

Explanation:

User vyatta is currently logged in to the system. The `show system login users` command displays active user login sessions, including the account name, terminal device, source location when available, and login time. The entry for `vyatta` shows a pseudo-terminal, `pts/0`, and a source address of `10.224.7.101`. A pseudo-terminal is allocated for an interactive remote terminal session, and its presence in this command's current-user listing establishes that the `vyatta` account has an active session on the router at the time the command was run. The timestamp provides the time at which that active session was established. This format follows the conventional Unix current-login reporting model, in which terminal and source-host fields identify active sessions rather than merely historical account activity. See the Linux who(1) manual page for the current-user session model and the VyOS system login documentation for related login and user-management behavior.

QUESTION NO: 5

vyatta@training:~$ show system commit

0 2013-05-03 21:07:54 by root via boot-config-loader

1 2013-05-03 00:05:32 by vyatta via cli

2 2013-05-02 23:15:23 by vyatta via cli

3 2013-04-08 17:57:48 by root via boot-config-loader

4 2013-03-12 18:08:45 by vyatta via cli

5 2013-01-22 22:56:04 by vyatta via cli

6 2012-11-04 02:36:36 by root via boot-config-loader

7 2012-10-12 16:15:36 by vyatta via cli

8 2012-10-11 16:23:08 by vyatta via cli

9 2012-09-10 18:51:06 by vyatta via cli

10 2012-09-04 23:56:28 by vyatta via cli

11 2012-08-31 23:25:35 by vyatta via cli

12 2012-08-31 23:08:05 by vyatta via cli

13 2012-08-31 23:07:32 by vyatta via cli

14 2012-08-31 23:06:56 by vyatta via cli

15 2012-08-31 03:38:53 by vyatta via cli

16 2012-08-31 03:37:15 by vyatta via cli

17 2012-08-31 03:03:53 by vyatta via cli

18 2012-06-22 04:58:47 by vyatta via cli

19 2012-06-20 19:48:08 by vyatta via cli

vyatta@training:~$

Based on the output, which two statements about this Brocade Vyatta vRouter are true? (Choose two.)

A. This vRouter has been upgraded three times

B. The administrator vyatta has read-write privileges to the device.

C. The last changes made to the device were made by the administrator vyatta.

D. The last changes saved on this system were saved on 2013-05-03.

ANSWER: B D

Explanation:

The administrator vyatta has read-write privileges to the device because the commit history records numerous configuration commits performed by that account “via cli.” In the Vyatta configuration model, a commit applies changes from the candidate configuration to the active configuration. Therefore, an account shown as the committing user demonstrably has authorization to make and commit configuration changes, rather than merely view operational information.

The last changes saved on this system were saved on 2013-05-03. Commit-history numbering is reverse chronological, with entry 0 representing the most recent commit event. Its timestamp is 2013-05-03 21:07:54. The recorded mechanism, boot-config-loader, identifies that the saved boot configuration was loaded during system startup, and that load is recorded as the latest configuration commit event. This output does not establish how many software upgrades occurred; boot-config-loader entries identify configuration loading at boot, not upgrades. Commit history is specifically intended to provide the ordering, time, user, and method associated with committed configuration revisions. See the Vyatta configuration and commit model in the Vyatta Configuration Mode documentation and the command reference material available from the Vyatta Documentation portal.

QUESTION NO: 6

Which two configuration elements are required when defining an eBGP neighbor? (Choose two.)

A. A local autonomous system number

B. A remote autonomous system number

C. An OSPF area number

D. A VLAN ID

ANSWER: A B

Explanation:

An eBGP configuration requires the local BGP autonomous system number and the remote autonomous system number configured for the neighbor. The local AS identifies the BGP process running on the vRouter. The remote AS identifies the autonomous system expected from the peer and distinguishes an external BGP session from an internal BGP session.

The neighbor address is also required to identify the peer, but it is represented by the BGP neighbor configuration node itself. For example, a configuration uses a local AS under `protocols bgp`, a neighbor address, and a `remote-as` value beneath that neighbor. BGP session establishment and AS-number handling are defined in RFC 4271. See also the VyOS BGP documentation.

QUESTION NO: 7

Which TCP destination port is normally used by HTTPS?

A. 21

B. 53

C. 80

D. 443

ANSWER: D

Explanation:

TCP port **443** is the well-known port normally assigned to HTTPS. HTTPS uses HTTP over TLS, allowing a client and server to protect application traffic with encryption, integrity checking, and server authentication.

A firewall rule permitting web access to an HTTPS server normally matches TCP protocol and destination port 443. The port assignment is listed in the IANA Service Name and Transport Protocol Port Number Registry.

QUESTION NO: 8

vyatta@training:~$ show system commit

0 2013-05-03 21:07:54 by root via boot-config-loader

1 2013-05-03 00:05:32 by vyatta via cli

2 2013-05-02 23:15:23 by vyatta via cli

3 2013-04-08 17:57:48 by root via boot-config-loader

4 2013-03-12 18:08:45 by vyatta via cli

5 2013-01-22 22:56:04 by vyatta via cli

6 2012-11-04 02:36:36 by root via boot-config-loader

7 2012-10-12 16:15:36 by vyatta via cli

8 2012-10-11 16:23:08 by vyatta via cli

9 2012-09-10 18:51:06 by vyatta via cli

10 2012-09-04 23:56:28 by vyatta via cli

11 2012-08-31 23:25:35 by vyatta via cli

12 2012-08-31 23:08:05 by vyatta via cli

13 2012-08-31 23:07:32 by vyatta via cli

14 2012-08-31 23:06:56 by vyatta via cli

15 2012-08-31 03:38:53 by vyatta via cli

16 2012-08-31 03:37:15 by vyatta via cli

17 2012-08-31 03:03:53 by vyatta via cli

18 2012-06-22 04:58:47 by vyatta via cli

19 2012-06-20 19:48:08 by vyatta via cli

vyatta@training:~$

Which two configuration elements are required in a source NAT masquerade rule? (Choose two.)

A. source address

B. protocol

C. translation address

D. outbound interface

ANSWER: C D

Explanation:

A source NAT masquerade rule requires a **translation address** configured as `masquerade` and an **outbound interface**. The translation setting identifies the NAT action: masquerade instructs the vRouter to replace the source address of matching outbound traffic with the current address assigned to the egress interface. This is particularly appropriate when that egress address is dynamically assigned, because the translated address follows any interface-address change automatically.

The outbound interface is required because it defines the egress path on which the source translation is applied and supplies the interface address used by masquerade. In the conventional Vyatta/Brocade NAT rule hierarchy, these settings are represented by commands such as `set service nat rule 10 outbound-interface eth0` and `set service nat rule 10 translation address masquerade`. Match criteria, including a source address or protocol, can be used to narrow the traffic selected by a rule, but masquerade operation fundamentally depends on the translation action and the specified egress interface. Current VyOS NAT documentation retains this same source-NAT model and describes masquerade as interface-based source translation. See the VyOS NAT44 documentation and the VyOS NAT configuration overview.

QUESTION NO: 9

You've configured a destination port in your firewall rule.

Which two additional elements are required in the rule? (Choose two.)

A. source port

B. action

C. protocol

D. destination address

ANSWER: B C

Explanation:

action and **protocol** are required when defining a firewall rule that matches a destination port. The action specifies the disposition that the vRouter must apply to packets that match the rule, such as accepting, dropping, or rejecting them. Without an explicit action, the rule has no defined packet-handling behavior.

A destination port is a transport-layer attribute, so the rule must also identify the applicable protocol. In practice, port matching is used with transport protocols such as TCP or UDP, and specifying the protocol tells the firewall how to interpret the port field in the packet. This makes the match unambiguous and ensures the rule is constructed as a valid protocol-aware firewall policy. For example, a rule permitting HTTPS traffic would pair destination port 443 with the TCP protocol and an accept action.

This follows the Vyatta/Brocade vRouter firewall rule model, in which rules combine match criteria with a mandatory packet action. See the Vyatta documentation portal for vRouter configuration material and the IANA Protocol Numbers registry for transport protocol identifiers used in IP packet processing.

QUESTION NO: 10

If all interfaces are active, which route would be preferred?

A. 10.1.1.0/24, administrative distance 110, learned through OSPF

B. 10.1.1.0/24, administrative distance 10, static route

C. 10.1.1.0/24, administrative distance 120, static route

D. 10.1.1.0/24, administrative distance 100, learned through OSPF

ANSWER: B

Explanation:

10.1.1.0/24, administrative distance 10, static route is preferred because all listed routes describe the identical destination prefix length, 10.1.1.0/24. After route lookup has identified equally specific prefix candidates, the router uses administrative distance to select the most trusted source of routing information. A lower administrative-distance value has greater preference. The static route has an explicitly configured distance of 10, which is lower than the distances of 100, 110, and 120 associated with the other candidate routes. Therefore, provided its next hop or outbound interface is active and the route is otherwise valid, it is installed as the active route for this prefix.

Administrative distance is a local route-selection attribute: it is not a metric exchanged by OSPF and does not represent path cost. It establishes which source is trusted when multiple sources offer routes to the same network. Once the route with administrative distance 10 is selected, traffic destined for addresses within 10.1.1.0/24 follows that static-route entry. General IP forwarding behavior, including use of the most-specific matching route, is described in RFC 1812; OSPF route processing and path selection are specified in RFC 2328.