

# DUMPSQUEEN

## Palo Alto Networks Certified Security Engineer (PCNSE) PAN-OS 11.0

Palo Alto Networks PCNSE

Version Demo

Total Demo Questions: 20

Total Premium Questions: 500

Buy Premium PDF

<https://dumpsqueen.com>

[support@dumpsqueen.com](mailto:support@dumpsqueen.com)

dumpsqueen.com

## QUESTION NO: 1

If a template stack is assigned to a device and the stack includes three templates with overlapping settings, which settings are published to the device when the template stack is pushed?

- A. The settings assigned to the template that is on top of the stack.
- B. The administrator will be prompted to choose the settings for that chosen firewall.
- C. All the settings configured in all templates.
- D. Depending on the firewall location, Panorama decides with settings to send.

**ANSWER: A**

## QUESTION NO: 2

What are three valid qualifiers for a Decryption Policy Rule match? (Choose three.)

- A. App-ID
- B. Custom URL Category
- C. User-ID
- D. Destination Zone
- E. Source Interface

**ANSWER: B C D**

### Explanation:

Reference: <https://docs.paloaltonetworks.com/pan-os/10-1/pan-os-admin/decryption/define-traffic-to-decrypt/create-a-decryption-policy-rule>

## QUESTION NO: 3

In a Panorama template, which three types of objects are configurable? (Choose three.)

- A. certificate profiles
- B. HIP objects
- C. QoS profiles

- D. security profiles
- E. interface management profiles

**ANSWER: B D E**

## QUESTION NO: 4

An administrator using an enterprise PKI needs to establish a unique chain of trust to ensure mutual authentication between Panorama and the managed firewalls and Log Collectors.

How would the administrator establish the chain of trust?

- A. Use custom certificates
- B. Enable LDAP or RADIUS integration
- C. Set up multi-factor authentication
- D. Configure strong password authentication

**ANSWER: A**

### Explanation:

Reference: [https://www.paloaltonetworks.com/documentation/80/panorama/panorama\\_adminguide/panorama-overview/plan-your-panorama-deployment](https://www.paloaltonetworks.com/documentation/80/panorama/panorama_adminguide/panorama-overview/plan-your-panorama-deployment)

## QUESTION NO: 5

A web server is hosted in the DMZ and the server is configured to listen for incoming connections on TCP port 443. A Security policies rule allowing access from the Trust zone to the DMZ zone needs to be configured to allow web-browsing access. The web server hosts its contents over HTTP(S). Traffic from Trust to DMZ is being decrypted with a Forward Proxy rule.

Which combination of service and application, and order of Security policy rules, needs to be configured to allow cJeartext web-browsing traffic to this server on tcp/443?

- A. Rule #1 application: web-browsing; service application-default; action: allow Rule #2- application: ssl; service: application-default; action: allow
- B. Rule #1: application; web-browsing; service: service-https; action: allow Rule #2 application: ssl; service: application-default, action: allow
- C. Rule #1: application: web-browsing; service: service-http; action: allow Rule #2: application: ssl; service: application-default; action: allow
- D. Rule #1 application: ssl; service: application-default; action: allow Rule #2 application; web-browsing; service application-default; action: allow

**ANSWER: B**

## QUESTION NO: 6

Panorama provides which two SD-WAN functions? (Choose two.)

- A. network monitoring
- B. control plane
- C. data plane
- D. physical network links

**ANSWER: B C**

## QUESTION NO: 7

What will be the egress interface if the traffic's ingress interface is ethernet1/6 sourcing from 192.168.111.3 and to the destination 10.46.41.113 during the time shown in the image?

```
admin@Lab33-111-PA-3060(active)> show clock
```

```
Thu Jun 8 12:49:55 PDT 2017
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 rulebase pbf rules test-pbf
```

```
test-pbf {  
  action {  
    forward {  
      egress-interface ethernet1/5;  
    }  
  }  
  from {  
    zone L3-Trust;  
  }  
  enforce-symmetric-return {  
    enabled no;  
  }  
  source 192.168.111.3;  
  destination 10.46.41.113;  
  source-user any;  
  application any;  
  service any;  
  schedule schedule-pbf;  
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)# show vsys vsys1 schedule schedule-pbf
```

```
schedule-pbf {  
  schedule-type {  
    recurring {  
      daily 16:00-21:00;  
    }  
  }  
}
```

```
#####
```

```
admin@Lab33-111-PA-3060(active)> show routing fib
```

id	destination	nexthop	flags	interface	mtu
47	0.0.0.0/0	10.46.40.1	ug	ethernet1/3	1500
67	10.10.20.0/24	0.0.0.0	u	ethernet1/7	1500
66	10.10.20.111/32	0.0.0.0	uh	ethernet1/7	1500
46	10.46.40.0/23	0.0.0.0	u	ethernet1/3	1500
49	10.46.44.0/23	0.0.0.0	u	ethernet1/5	1500
45	10.46.41.111/32	0.0.0.0	uh	ethernet1/3	1500
70	10.46.41.113/32	10.46.40.1	ug	ethernet1/3	1500
48	10.46.45.111/32	0.0.0.0	uh	ethernet1/5	1500
51	192.168.111.0/24	0.0.0.0	u	ethernet1/6	1500
50	192.168.111.2/32	0.0.0.0	uh	ethernet1/6	1500

- A. ethernet1/7
- B. ethernet1/5
- C. ethernet1/6
- D. ethernet1/3

**ANSWER: D**

## QUESTION NO: 8

For which two reasons would a firewall discard a packet as part of the packet flow sequence? (Choose two.)

- A. ingress processing errors
- B. rule match with action “deny”
- C. rule match with action “allow”
- D. equal-cost multipath

**ANSWER: A B**

## QUESTION NO: 9

Decrypted packets from the website <https://www.microsoft.com> will appear as which application and service within the Traffic log?

- A. web-browsing and 443
- B. SSL and 80
- C. SSL and 443
- D. web-browsing and 80

**ANSWER: C**

## QUESTION NO: 10

When overriding a template configuration locally on a firewall, what should you consider?

- A. Panorama will update the template with the overridden value.
- B. The firewall template will show that it is out of sync within Panorama.
- C. Only Panorama can revert the override.
- D. Panorama will lose visibility into the overridden configuration.

**ANSWER: B**

## QUESTION NO: 11

An engineer is tasked with enabling SSL decryption across the environment. What are three valid parameters of an SSL Decryption policy? (Choose three.)

- A. URL categories
- B. source users
- C. source and destination IP addresses
- D. App-ID
- E. GlobalProtect HIP

**ANSWER: A B C**

## QUESTION NO: 12

The same route appears in the routing table three times using three different protocols Which mechanism determines how the firewall chooses which route to use?

- A. Administrative distance
- B. Round Robin load balancing
- C. Order in the routing table
- D. Metric

**ANSWER: A**

### Explanation:

Administrative distance is the measure of trustworthiness of a routing protocol. It is used to determine the best path when multiple routes to the same destination exist. The route with the lowest administrative distance is chosen as the best route.

When the same route appears in the routing table three times using three different protocols, the mechanism that determines which route the firewall chooses to use is the administrative distance. This is explained in the Palo Alto Networks PCNSE Study Guide in Chapter 6: Routing, under the section "Route Selection":

"Administrative distance is a value assigned to each protocol that the firewall uses to determine which route to use if multiple protocols provide routes to the same destination. The route with the lowest administrative distance is preferred."

## QUESTION NO: 13

Which three items are import considerations during SD-WAN configuration planning? (Choose three.)

- A. link requirements
- B. the name of the ISP
- C. IP Addresses

D. branch and hub locations

**ANSWER: A C D**

**Explanation:**

<https://docs.paloaltonetworks.com/sd-wan/1-0/sd-wan-admin/sd-wan-overview/plan-sd-wan-configuration>

## QUESTION NO: 14 - (DRAG DROP)

DRAG DROP

Below are the steps in the workflow for creating a Best Practice Assessment in a firewall and Panorama configuration. Place the steps in order.

**Select and Place:**

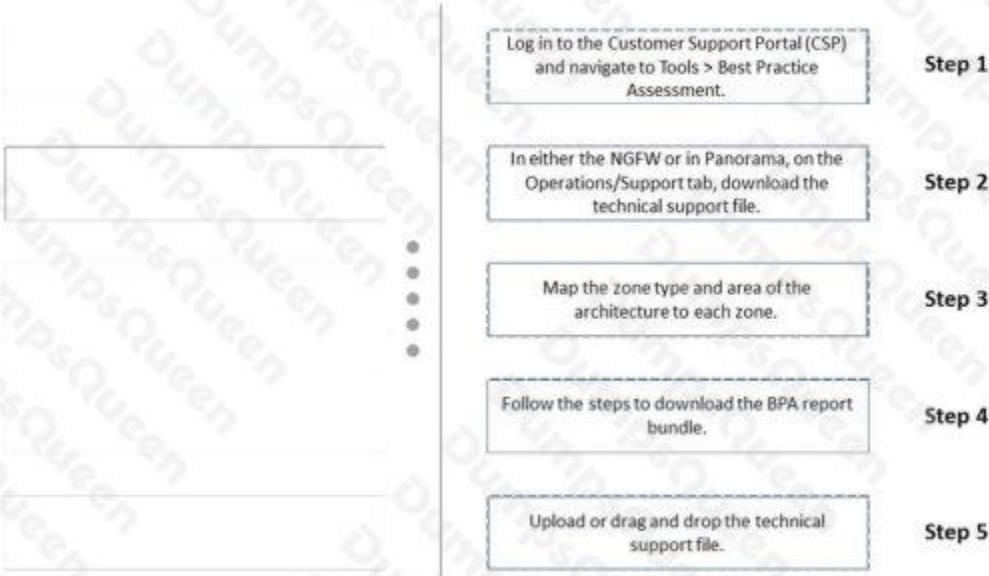
**Answer Area**

In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.		<b>Step 1</b>
Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.		<b>Step 2</b>
Upload or drag and drop the technical support file.		<b>Step 3</b>
Map the zone type and area of the architecture to each zone.		<b>Step 4</b>
Follow the steps to download the BPA report bundle.		<b>Step 5</b>

**ANSWER:**



## Answer Area

- 
- Step 1: Log in to the Customer Support Portal (CSP) and navigate to Tools > Best Practice Assessment.
  - Step 2: In either the NGFW or in Panorama, on the Operations/Support tab, download the technical support file.
  - Step 3: Map the zone type and area of the architecture to each zone.
  - Step 4: Follow the steps to download the BPA report bundle.
  - Step 5: Upload or drag and drop the technical support file.

Explanation:

**QUESTION NO: 15**

An engineer configures SSL decryption in order to have more visibility to the internal users' traffic when it is regressing the firewall.

Which three types of interfaces support SSL Forward Proxy? (Choose three.)

- A. High availability (HA)
- B. Layer
- C. Virtual Wire
- D. Tap
- E. Layer 3

**ANSWER: B C E**

Explanation:

[SSL Forward Proxy](#) is a feature that allows the firewall to decrypt and inspect outbound SSL traffic from internal users to external servers<sup>1</sup>. The firewall acts as a proxy (MITM) generating a new certificate for the accessed URL and presenting it to the client during SSL handshake<sup>2</sup>.

[SSL Forward Proxy can be configured on any interface type that supports security policies, which are Layer 2, Virtual Wire, and Layer 3 interfaces](#)<sup>1</sup>. These interface types allow the firewall to apply security profiles and URL filtering on the decrypted SSL traffic.

## QUESTION NO: 16

An administrator has two pairs of firewalls within the same subnet. Both pairs of firewalls have been configured to use High Availability mode with Active/Passive. The ARP tables for upstream routes display the same MAC address being shared for some of these firewalls.

What can be configured on one pair of firewalls to modify the MAC addresses so they are no longer in conflict?

- A. Configure a floating IP between the firewall pairs.
- B. Change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet.
- C. Change the interface type on the interfaces that have conflicting MAC addresses from L3 to VLAN.
- D. On one pair of firewalls, run the CLI command: set network interface vlan arp.

## ANSWER: B

### Explanation:

<https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000Cm1OCAS>

change the Group IDs in the High Availability settings to be different from the other firewall pair on the same subnet. This will prevent the MAC addresses from conflicting and allow the firewalls to properly route traffic. You can also configure a floating IP between the firewall pairs if necessary.

## QUESTION NO: 17

Which three statements correctly describe Session 380280? (Choose three.)

```
> show session id 380280
Session                               380280
c2s flow:
source:                               172.17.149.129 [L3-Trust]
dst:                                   104.154.09.105
proto:                                 6
sport:                                60997      dport:     443
state:                                ACTIVE     type:      FLOW
src user:                              unknown
dst user:                              unknown

s2c flow:
source:                               104.154.89.105 [L3-Untrust]
dst:                                   10.46.42.149
proto:                                 6
sport:                                443      dport:     7260
state:                                ACTIVE     type:      FLOW
src user:                              unknown
dst user:                              unknown

start time                            : Tue Feb 9 20:38:42 2021
timeout                               : 15 sec
time to live                           : 2 sec
total byte count (c2s)                 : 3330
total byte count (s2c)                 : 12698
layer7 packet count (c2s)              : 14
layer7 packet count (s2c)              : 19
vsys                                    : vsys1
application                            : web-browsing
rule                                    : Trust-to-Untrust
service timeout override (index)       : False
session to be logged at end             : True
session in session ager                 : True
session updated by HA peer              : False
session proxied                         : True
address/port translation                : source
nat-rule                                : Trust-NAT (vsys1)
Layer7 processing                       : Completed
URL filtering enabled                   : True
URL category                            : computer-and-internet-info, low-risk
session via syn-cookies                  : False
session terminated on host               : False
session traverses tunnel                 : False
session terminate tunnel                 : False
captive portal session                   : False
ingress interface                       : ethernet1/6
egress interface                        : ethernet1/3
session GOS rule                        : N/A (class 4)
tracker stage l7proc                    : proxy timer expired
end-reason                              : unknown
```

- A. The application was initially identified as "ssl."
- B. The session has ended with the end-reason "unknown."
- C. The session did not go through SSL decryption processing.
- D. The application shifted to "web-browsing."
- E. The session went through SSL decryption processing.

**ANSWER: B D E**

## QUESTION NO: 18

Which option describes the operation of the automatic commit recovery feature?

- A. It enables a firewall to revert to the previous configuration if rule shadowing is detected.
- B. It enables a firewall to revert to the previous configuration if application dependency errors are found.
- C. It enables a firewall to revert to the previous configuration if a commit causes HA partner connectivity failure.
- D. It enables a firewall to revert to the previous configuration if a commit causes Panorama connectivity failure.

ANSWER: D

**Explanation:**

Reference: <https://docs.paloaltonetworks.com/pan-os/9-1/pan-os-new-features/panorama-features/automatic-panorama-connection-recovery.html>

## QUESTION NO: 19

**QoS Profile**

Profile Name: General-QoS

Egress Max: 1000

Egress Guaranteed: 0

Class Bandwidth Type:  Mbps  Percentage

CLASS	PRIORITY	EGRESS MAX (MBPS)	EGRESS GUARANTEED (MBPS)
class1	low	0	100
class2	medium	0	400
class3	high	0	400
class4	real-time	0	100

+ Add - Delete

class 4 is the default class

NAME	Source		Destination		APPLICATION	SERVICE	DSCP/TOS	CLASS
	ZONE	ADDRESS	ZONE	ADDRESS				
1 Class-1Apps	any	any	INTERNET	any	smtp, ssh, telnet	any	any	1
2 Class-2Apps	any	any	INTERNET	any	google-meet, webex, zoom	any	any	2
3 Class-3Apps	any	any	INTERNET	any	dns, google-video, youtube-stre...	any	any	3
4 Class-4Apps	any	any	INTERNET	any	facetime	any	any	4

View the screenshots. A QoS profile and policy rules are configured as shown. Based on this information, which two statements are correct? (Choose two.)

- A. DNS has a higher priority and more bandwidth than SSH.
- B. Google-video has a higher priority and more bandwidth than WebEx.
- C. SMTP has a higher priority but lower bandwidth than Zoom.
- D. Facetime has a higher priority but lower bandwidth than Zoom.

**ANSWER: C D**

### QUESTION NO: 20

An administrator logs in to the Palo Alto Networks NGFW and reports that the WebUI is missing the Policies tab.

Which profile is the cause of the missing Policies tab?

- A. Admin Role
- B. WebUI
- C. Authentication
- D. Authorization

**ANSWER: A**