Vendor: Juniper

Exam Code: JN0-533

Exam Name: FWV, Specialist (JNCIS-FWV)

Version: Demo

Exam A

QUESTION 1
Your ScreenOS device does not have a static IP address. You want to be able to access it using its FQDN. How would you implement this task?

A. Configure a domain in DNS.
B. Configure syslog.
C. Configure SNMP.
D. Configure DDNS.

Correct Answer: D

QUESTION 2
You have just installed a new ScreenOS device in your network and you want only a select range of IP addresses to have administrative access to the device. Which choice will allow you to accomplish this?

A. Configure a manager IP.
B. Configure the management interface.
C. Configure a management IP on the trust interface.
D. Configure new system administrators.

Correct Answer: A

QUESTION 3
A routing table contains an IBGP route for 192.168.0.0/24, a RIP route for 192.168.0.0/23, an OSPF route for 192.168.0.0/22, and a static route for 192.168.0.0/16. When the router receives traffic destined for 192.168.0.1, which route will the router use?

A. the IBGP route
B. the OSPF route
C. the RIP route
D. the static route

Correct Answer: A

QUESTION 4
You are troubleshooting telnet traffic destined to IP address 10.10.10.1. You decide to run debug and want to set the flow filter. Which command will show only the telnet traffic going to the 10.10.10.1 address?

A. ssg5-serial-> set ffilter dst-ip 10.10.10.1
   ssg5-serial-> set ffilter dst-port 23
B. ssg5-serial-> set ffilter dst-ip 10.10.10.1 dst-port 23
C. ssg5-serial-> set ffilter dst-port 23
D. ssg5-serial-> set ffilter dst-ip 10.10.10.1

Correct Answer: B

QUESTION 5

You have enabled BGP on your ScreenOS device and configured a single EBGP peer. The CLI shows that the BGP connection is transitioning between the CONNECT and ACTIVE states, but never reaching the ESTABLISHED state. What are three reasons for this behavior? (Choose three.)

A. The peer is blocking traffic destined for TCP port 179.
B. The peer address is not configured correctly.
C. The enable statement has not been configured for the peer.
D. The peer AS number is not configured correctly.
E. BGP has not been enabled on the virtual router.

Correct Answer: ABD

QUESTION 6
You want to set up a last resort route and prevent route lookups in either the source-based routing table or the destination-based routing table. What should you do?

A. Disable SIBR and create a default route in the trust-vr table using the null interface as the outgoing interface with a higher metric than other routes.
B. Disable SIBR and create a default route in the trust-vr table using the null interface as the outgoing interface with a lower metric than other routes.
C. Enable SIBR and create a default route in the SIBR table using the null interface as the outgoing interface with a higher metric than other routes.
D. Enable SIBR and create a default route in the SIBR table using the null interface as the outgoing interface with a lower metric than other routes.

Correct Answer: C

QUESTION 7
You have the following BGP configuration in place to establish a session with a remote peer over your ethernet4 interface.

set vrouter trust-vr protocol bgp 65000
set vrouter trust-vr protocol bgp enable
set vrouter trust-vr protocol bgp neighbor remote-as 65500 set vrouter trust-vr protocol bgp neighbor enable

Which additional statement is necessary to establish the session?

A. set interface protocol bgp enable
B. set interface ethernet4 bgp enable
C. set vrouter trust-vr protocol bgp interface ethernet4
D. set interface ethernet4 protocol bgp

Correct Answer: D

QUESTION 8

You have only one public IP address available and you must allow external access to three servers on a DMZ network. Which two NAT types would allow you to accomplish your objective? (Choose two.)

A. MIP
B. VIP
C. NAT-dst
D. NAT-src

Correct Answer: BC

QUESTION 9
Your ScreenOS device is configured with multiple NAT types.
What is the order of precedence in this situation?

A. interface-based NAT -> VIP -> MIP -> policy-based NAT
B. VIP -> MIP -> policy-based NAT -> interface-based NAT
C. MIP -> VIP -> interface-based NAT -> policy-based NAT
D. MIP -> VIP -> policy-based NAT -> interface-based NAT

Correct Answer: D

QUESTION 10
You must translate a range of public IP addresses to a range of internal IP addresses. Which two mechanisms would you use to accomplish your objective? (Choose two.)

A. MIP using masks
B. VIP using masks
C. policy-based NAT-dst
D. policy-based NAT-src

Correct Answer: AC

QUESTION 11
Your ScreenOS device is using NAT. Which NAT function allows you to use a single IP address from an untrust zone to communicate to multiple IP addresses in a trust zone?

A. NAT-src with PAT enabled
B. NAT-dst with PAT enabled
C. NAT-src using a DIP pool with PAT enabled
D. NAT-dst using a DIP pool with PAT disabled

Correct Answer: B

QUESTION 12

Which two statements are true about NAT? (Choose two.)

A. Managed IP is one-to-one address mapping for bidirectional access.
B. Mapped IP is one-to-one address mapping for bidirectional access.
C. Dynamic IP is the public address that can be used for external access to your Web server.
D. Dynamic IP is the public address that internal users can use to access the Internet.

Correct Answer: BD

QUESTION 13
Which NAT has bidirectional translation by default?

A. NAT-src
B. NAT-dst
C. VIP
D. MIP

Correct Answer: D

QUESTION 14
You are using interface-based NAT for traffic passing from the trust zone to the untrust zone.
What will occur?

A. The source IP address is not translated.
B. The source IP address is translated to the trust interface IP address.
C. The network address and port translation (NAPT) is performed on the loopback interface.
D. The source IP address is translated to the untrust interface IP address.

Correct Answer: D

QUESTION 15
You have configured a single-port VIP to forward HTTP traffic from the untrust interface on your ScreenOS device to an internal Web server. You have configured a policy to allow this traffic. Traffic from the untrust interface that matches this policy is unable to connect to the Web server.
What is a solution to this problem?

A. You must reboot the ScreenOS device for the VIP to become active.
B. You must ensure the ScreenOS device has a route to the Web server.
C. You must ensure the Web server is directly connected to the ScreenOS device.
D. You must save the ScreenOS device configuration for the VIP to become active.

Correct Answer: B

QUESTION 16

You must verify on your ScreenOS device that you have configured the correct tunnel peer and determine which IKE proposals the remote device is sending and accepting. Which command should you use?

A. get ike gateway
B. get ike peer
C. get sa active
D. get ike active

Correct Answer: A

QUESTION 17

You are building an IPsec VPN and want to authenticate and encrypt the content. Which two Phase 1/ Phase 2 (P1/P2) proposals would achieve this goal? (Choose two.)

A. P1: pre-g5-3des-sha, P2: g5-esp-3des-sha
B. P1: pre-g2-aes128-sha, P2: g5-ah-aes128-sha
C. P1: pre-g5-des-md5, P2: g5-ah-des-md5
D. P1: pre-g2-esp128-sha, P2: g2-esp-aes128-sha

Correct Answer: AD

QUESTION 18
You are configuring a VPN with IKE between headquarters and a branch office that uses a dynamic public IP address. Which IKE mode should you use?

A. quick mode
B. main mode
C. aggressive mode
D. wizard mode

Correct Answer: C

QUESTION 19
Which two statements are true about policy-based VPNs as compared to route-based IPsec VPNs when using ScreenOS devices? (Choose two.)

A. For policy-based IPsec VPNs, you can configure 0.0.0.0/0 as the proxy ID on both VPN gateways regardless of the security policy.
B. For route-based IPsec VPNs, you can configure 0.0.0.0/0 as the proxy ID on both VPN gateways regardless of the security policy.
C. For route-based IPsec VPNs, the proxy ID is derived from the policy.
D. For policy-based IPsec VPNs, the proxy ID is derived from the policy.

Correct Answer: BD

QUESTION 20
You want to ensure that the IKE Phase 2 key is totally independent of the IKE Phase 1 key. Which IKE feature would you enable?

A. Perfect Forward Secrecy
B. Diffie-Hellman Group 5
C. Replay Protection
D. Rekey Protection

Correct Answer: A

QUESTION 21
Which two Diffie-Hellman (DH) groups are supported by ScreenOS software? (Choose two.)

A. DH Group 1: 1024-bit
B. DH Group 2: 1024-bit
C. DH Group 5: 1536-bit
D. DH Group 15: 2048-bit

Correct Answer: BC

QUESTION 22
How is a route-based VPN different from a policy-based VPN?

A. A route-based VPN requires manual keys for encryption and authentication.
B. A route-based VPN requires static route entries for the remote peer.
C. A route-based VPN is bound to a tunnel interface.
D. A route-based VPN is bound to a loopback interface.

Correct Answer: C

QUESTION 23
Which two statements are true about VPN Monitor on a ScreenOS device? (Choose two.)

A. With a route-based VPN failure, VPN Monitor marks the tunnel interface status as down.
B. With a policy-based VPN failure, VPN Monitor marks the tunnel interface status as down.
C. VPN Monitor uses UDP to detect a VPN connection failure.
D. VPN Monitor uses ICMP to detect a VPN connection failure.

Correct Answer: AD

QUESTION 24
Which two authentication algorithms does AutoKey IKE use during Phase 1 negotiations? (Choose two.)

A. AES-256
B. SHA2-256
C. MD5
D. 3DES

Correct Answer: BC

QUESTION 25
You are receiving 3000 SYN packets per second from multiple outside sources to the same destination IP address in your network. You want the SYN proxy Screen option to engage when SYN packets exceed 2000 per second, but the SYN proxy is not engaging. What is causing the problem?

A. The SYN packets are being sent to multiple destination ports.
B. The alarm threshold is too high.
C. The destination threshold is too high.
D. The option to only generate alarms without dropping packets is set to ON.

Correct Answer: A

QUESTION 26
You have configured deep-packet inspection on a ScreenOS device. You have not modified the default threshold values. The device detects a single session that matches an attack. Which two actions can you configure the device to take? (Choose two.)

A. Close the connection and disallow further connections from the client to the server.
B. Close the connection and rate-limit further connections to the server.
C. Discard all additional packets related to the session.
D. Send a TCP RST message to both the client and server.

Correct Answer: CD

QUESTION 27
A ScreenOS device detects a large number of sessions that match the same deep inspection attack object. What are two ways to configure the device? (Choose two.)

A. Activate dynamic firewall policies.
B. Close the connection and disallow further connections from the client.
C. Close the connection and rate-limit further connections to the server.
D. Log an alert.

Correct Answer: BD

QUESTION 28
The ScreenOS software performs virus scanning for which three protocols? (Choose three.)

A. FTP
B. HTTP
C. HTTPS
D. NetBIOS
E. SMTP

Correct Answer: ABE

QUESTION 29
You have configured integrated Web filtering in the ScreenOS software. A URL appears in the blacklist, the whitelist, and a user-defined category. Additionally, the device can obtain categorization information from the SurfControl server. Which configuration will the device use to determine the action to take for Web requests for the URL?

A. the blacklist
B. the SurfControl categorization
C. the user-defined category
D. the whitelist

Correct Answer: A

QUESTION 30
You have configured integrated Web filtering in the ScreenOS software. You find that users trying to access http://www.example.com are being blocked by your Web-filtering configuration. However, you want all users to be able to access this Web site. What are two methods to allow this traffic? (Choose two.)

A. Configure an SC-CPA exception for the URL.
B. Configure the URL as part of a custom category and allow requests in that category.
C. Configure the URL as part of the blacklist.
D. Configure the URL as part of the whitelist.

Correct Answer: BD

QUESTION 31
You want to enable the integrated Web-filtering feature on a ScreenOS device.
Which Web-filtering technology would be used?

A. WebSense
B. McAfee
C. Symantec
D. SurfControl

Correct Answer: D

QUESTION 32
Which two statements are correct about internal antivirus scanning? (Choose two.)

A. It includes a predefined file extension list for each protocol.
B. It allows you to load-balance ICAP scan servers.
C. It requires you to install a ScreenOS software license.
D. It provides inbound spyware and phishing protection.

Correct Answer: CD

QUESTION 33
You want to copy an external configuration file to your ScreenOS device and have it become active only after the device reboots. How would you accomplish this goal?

A. From the device, copy the configuration from an external TFTP server to the device's flash memory.
B. From the device, copy the configuration from an external TFTP server to the device's RAM.
C. From the device, copy the configuration from an external TFTP server and merge it with the current configuration.
D. From the device, copy the configuration from the device's flash memory to an external TFTP server.

Correct Answer: A

QUESTION 34
You want to ensure that the ScreenOS device sends alert data to notify the security operation center. Which three log destinations would you set to accomplish your objective? (Choose three.)

A. e-mail
B. SNMP
C. console
D. internal
E. syslog

Correct Answer: ABE

QUESTION 35
You want to know the username and IP address of users who logged in to the WebUI. In which log would you find this information?

A. admin log
B. event log
C. traffic log
D. self log

Correct Answer: B

QUESTION 36
You manage a ScreenOS device. A user complains that the FTP download speed is slow. You suspect a cable or an interface might be the problem. Which command provides interface error information?

A. show counter flow interface
B. get counter flow interface
C. show counter statistics interface
D. get counter statistics interface

Correct Answer: D

QUESTION 37
You want to centralize the logging for all your ScreenOS devices and you must be able to synchronize the log. Which two actions would you perform to accomplish this? (Choose two.)

A. Enable logging to the console.
B. Enable logging to syslog.
C. Enable NTP and set to UTC/GMT time.
D. Enable logging to the USB.

Correct Answer: BC

QUESTION 38
You have lost the admin user password for your NetScreen device. No other user accounts are configured on the device. How would you access the CLI?

A. Log in on the console using the secret name "recovery" and password "netscreen".
B. Send a break to the console during the boot process and modify the configuration registers.
C. Log in on the console using the serial number as the username and password.
D. Log in on the console using the secret name "recovery" and the serial number as the password.

Correct Answer: C

QUESTION 39
You are the administrator of a NetScreen 5GT. The system administrator cannot use SSH to log in to the NetScreen 5GT. Referring to the exhibit, what is the problem?

```
SSH V2 is active
ns5gt-> get int et1
Interface ethernet1:
description ethernet1
number 2, if_info 176, if_index 0, mode nat
link up, phy-link up/full-duplex
status change:1, last change:02/06/1997 18:02:32
vsys Root, zone Trust, vr trust-vr
dhcp client disabled
PPPoE disabled
```

admin mtu 0, operating mtu 1500, default mtu 1500
*ip 192.168.1.1/24
*manage ip 192.168.1.1,
route-deny disable
pmtu-v4 disabled
ping enabled, telnet enabled, SSH enabled, SNMP enabled
web enabled, ident-reset disabled, SSL enabled
SSH is enabled
SSH is ready for connections
Maximum sessions: 3
Active sessions: 3

A. Interface eth1 does not permit logins using SSH.
B. SSH is not enabled on the NetScreen 5GT.
C. Interface eth1's link status is down.
D. The maximum SSH session has been used.

Correct Answer: D

QUESTION 40
User1 wants to create the policy in the ScreenOS device, but is not successful.
Referring to the exhibit, what is the problem?

set admin name "admin"
set admin password "nOsYMqrbAs/McFsJrs6HwcIt3AF6yn"
set admin user "User1" password "nLZwKErINPPCcphC6sFMXrJ" privilege "read-only"
set admin port 8080
set admin access attempts 5
set admin access lock-on-failure 5
set admin auth web timeout 10
set admin auth server "Local"

A. The User1 account has been suspended.
B. User1 does not have any account in this device.
C. User1 logged in to the device with wrong port.
D. User1 does not have the proper permission to create a policy.

Correct Answer: D

QUESTION 41
You are the administrator of a NetScreen 5GT. For troubleshooting purposes, you must be able to ping untrusted interfaces.
Referring to the exhibit, how do you enable ping for interface eth2?

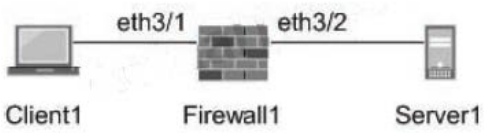
ns5gt-> get int eth2
Interface ethernet2:
description ethernet2
number 8, if_info 704, if_index 0, mode route
link up, phy-link up/full-duplex
status change:7, last change:09/26/2012 23:08:22
vsys Root, zone Untrust, vr trust-vr
dhcp client disabled
PPPoE disabled

admin mtu 0, operating mtu 1500, default mtu 1500
*ip 171.211.111.111/30 mac 0014.f693.edc8
*manage ip 171.211.111.111, mac 0014.f693.edc8
route-deny disable
pmtu-v4 disabled
ping disabled, telnet enabled, SSH disabled, SNMP disabled web enabled, ident-reset disabled, SSL disabled
DNS Proxy disabled, webauth disabled, g-arp enabled, webauth-ip 0.0.0.0 OSPF disabled BGP disabled
RIP disabled RIPng disabled mtrace disabled PIM: not configured IGMP not configured
MLD not configured
NHRP disabled
bandwidth: physical 100000kbps, configured egress [gbw 0kbps mbw 0kbps] configured ingress mbw 0kbps, current bw 0kbps
total allocated gbw 0kbps
DHCP-Relay disabled at interface level
DHCP-server disabled

A. ns5gt-> unset int eth2 manage-ip ping
B. ns5gt-> set int eth2 manage ping
C. ns5gt-> enable int eth2 manage ping
D. ns5gt-> set int eth2 manage-ip ping

Correct Answer: B

QUESTION 42
In the exhibit, eth3/1 is in the client-vr virtual router and eth3/2 is in the server-vr virtual router. Your policies permit all traffic between all zones. You want to ensure Client1 can contact Server1. In this scenario, which two statements are true? (Choose two.)



A. By default, all interface routes are automatically imported into all virtual routers.
B. You can configure a static route for Server1 in the client-vr virtual router that points to eth3/2.
C. You can configure a static route for Server1 in the client-vr virtual router that points to the server-vr virtual router.
D. You can configure a route export policy to export the route for Server1 to the client-vr virtual router.

Correct Answer: CD

QUESTION 43
Referring to the output shown in the exhibit, which NAT configuration is being used?

```
ns5gt-> get int

Interfaces in vsys Root:
Name            IP Address                          Zone        MAC             VLAN State VSD
eth1            192.168.1.1/24                      Trust       0014.f693.edc2    -    U   -
eth2            2.2.2.2/30                          Untrust     0014.f693.edc8    -    U   -

ns5gt-> get db stream
ipid = 19121(4ab1), @05a00214
  packet passed sanity check.
  flow_decap_vector IPv4 process
  ethernet2:1.1.1.1/55308->2.2.2.2/90,6<Root>
  no session found
  flow_first_sanity_check: in <ethernet2>, out <N/A>
  self check, not for us
  chose interface ethernet2 as incoming nat if.
  flow_first_routing: in <ethernet2>, out <N/A>
  search route to (ethernet2, 1.1.1.1->192.168.1.4) in vr trust-vr for vsd-0/flag-0/ifp-null
  [ Dest] 1.route 192.168.1.4->192.168.1.4, to ethernet1
  routed (x_dst_ip 192.168.1.4) from ethernet2 (ethernet2 in 0) to ethernet1
  policy search from zone 1-> zone 2
 policy_flow_search  policy search nat_crt from zone 1-> zone 10
  RPC Mapping Table search returned 0 matched service(s) for (vsys Root, ip 2.2.2.2, port 90, proto 6)
  No SW RPC rule match, search HW rule
  swrs_search_ip: policy matched id/idx/action = 24/0/0x9
    Permitted by policy 24
    post addr xlation: 1.1.1.1->192.168.1.4.
```

A. interface-based NAT
B. DIP
C. source-based NAT
D. VIP

Correct Answer: D

Explanation:

You can see packet originally aimed at 2.2.2.2 and then the destination changes to 192.168.1.4

QUESTION 44
Referring to the exhibit, what does the log show?

```
ns5-> get session

if 2(nspflag 800801):192.168.1.11/49237->74.125.235.48/443,6,a4badbf6bc41,sess token 3,vlan 0,tun 0,vsd 0,route
1,wsf 6
 if 8(nspflag 10800800):173.209.131.114/1034<-74.125.235.48/443,6,00222d52786c,sess token 4,vlan 0,tun 0,vsd
0,route 7,wsf 2
id 1568/s**,vsys 0,flag 00000000/0000/0001,policy 1,time 26, dip 2 module 0
 if 2(nspflag 800801):192.168.1.113/53514->123.176.112.241/80,6,842b2b91c303,sess token 3,vlan 0,tun 0,vsd
0,route 1,wsf 0
 if 8(nspflag 10800800):173.209.131.114/2120<-123.176.112.241/80,6,00222d52786c,sess token 4,vlan 0,tun 0,vsd
0,route 7,wsf 2
id 1571/s**,vsys 0,flag 00000000/0000/0001,policy 1,time 178, dip 2 module 0
```

A. The device is using VIP.
B. The device is using DIP ID 4.
C. The device is using source NAT.
D. The device is using destination NAT.

Correct Answer: C

Explanation:
The source IP of the outgoing packets is not the same as the destination IP of the incoming responses.

QUESTION 45
Referring to the exhibit, what is the appropriate VPN monitor status?

```
isg1000-> get sa active
Total active sa: 1
HEX ID    Gateway         Port Algorithm     SPI   Life:sec kb Sta   PID vsys0001001a<   192.168.1.1  500
esp:3des/sha1 d4cfbfd6  1678 unlim A/-    -1 1
```

A. The VPN is active and the peer is down.
B. The VPN is active and VPN Monitor is not configured for the peer.
C. The VPN is active and the peer is up.
D. The VPN is inactive and VPN Monitor is not configured for the peer.

Correct Answer: B

Explanation:
"A/-" shows the VPN active, but monitor is unavailable (likely because the other end is not a screenOS device)

QUESTION 46
What is shown in the exhibit?

```
ssg20-> get policy
Total regular policies 2, Default deny, Software based policy search, new policy enabled.
    ID From     To       Src-address  Dst-address  Service              Action State   ASTLCB
     1 Trust    Untrust  trust-local  vpn-remote   ANY                  Tunnel enabled -----X
     3 Untrust  Trust    vpn-remote   trust-local  ANY                  Tunnel enabled -----X
```

A. a route-based VPN
B. a global policy
C. a policy-based VPN
D. a policy with counting enabled

Correct Answer: C

Explanation:
The "Tunnel" action is specific to policy-based VPN

QUESTION 47
The exhibit displays output from the event log of a ScreenOS device. Given the information shown in the exhibit, which two statements are correct? (Choose two.)

```
ssg20-> get log event
Total event entries = 40
Date       Time     Module Level  Type Description
2012-11-27 02:33:58 system info  00536 IKE 192.168.1.4 Phase 2 msg ID
                                       d85b5a89: Negotiations have failed.
2012-11-27 02:33:58 system info  00536 Rejected an IKE packet on ethernet0/0
                                       from 192.168.1.4:500 to 192.168.1.10:
                                       500 with cookies e14eb84bcfcfba09 and
                                       94060dc9f2ad72e3 because The peer sent
                                       a proxy ID that did not match the one
                                       in the SA config.
2012-11-27 02:33:58 system info  00536 IKE 192.168.1.4 Phase 2: No policy
                                       exists for the proxy ID received:
                                       local ID (10.20.1.0/255.255.255.0, 17,
                                       53) remote ID (10.204.1.0/255.255.255.0,
                                       17, 53).
2012-11-27 02:33:58 system info  00536 IKE 192.168.1.4 Phase 2 msg ID
                                       d85b5a89: Responded to the peer's
                                       first message.
```

A. The VPN initiator is sending a proxy ID of:
   local: 10.20.1.0/24 remote:10.204.1.0/24
   service:ANY
B. The VPN contains a proxy ID mismatch.
C. Phase 2 negotiations completed successfully.
D. Phase 1 negotiations completed successfully.

Correct Answer: BD

QUESTION 48
Which two statements are true about the exhibit? (Choose two.)

```
ssg20-> get ike cookies

IKEv1 SA -- Active: 1, Dead: 0, Total 1

80522f/0003, 192.168.1.10:500->192.168.1.4:500,
PRESHR/grp5/AES256/SHA, xchg(2) (ns204/grp-1/usr-1)
resent-tmr 322 lifetime 28800 lt-recv 28800 nxt_rekey 28796
cert-expire 0
initiator, err cnt 0, send dir 0, cond 0x0
nat-traversal map not available
ike heartbeat               : disabled
ike heartbeat last rcv time: 0
ike heartbeat last snd time: 0
XAUTH status: 0
DPD seq local 0, peer 0


IKEv2 SA -- Active: 0, Dead: 0, Total 0
```

A. It contains information regarding Phase 1 of IPsec.
B. It contains information regarding Phase 2 of IPsec.
C. The VPN is using certificates.
D. The VPN is using preshared keys.

Correct Answer: AD

QUESTION 49
Referring to the exhibit, which three statements are true? (Choose three.)

NS5200(M)-> get nsrp
nsrp version: 2.0
cluster info:
cluster iD. 1, namE. 5200
local unit iD. 8000208
active units discovereD.
index: 0, unit iD. 8014208, ctrl maC. 0010db000085, data maC.
0010db000086
index: 1, unit iD. 8337344, ctrl maC. 0010db0000c5, data maC.
0010db0000c6
total number of units: 2
VSD group info:
init hold timE. 5
heartbeat lost thresholD. 3
heartbeat interval: 200(ms)
master always exist: enabled
group priority preempt holddown inelig master PB other members 0 50 yes 45 no myself 8330044
total number of vsd groups: 1
Total iteration= ,time=878546093,max=4900,min=170,average=18 RTO mirror info:

run time object synC. enabled
ping session synC. enabled
coldstart sync done
nsrp data packet forwarding is enabled
nsrp link info:
control channel: ha1 (ifnum: 5) maC. 0010db000085 statE. up data channel: ha2 (ifnum: 6) maC. 0010db000086 statE. up
ha secondary path link not available
NSRP encryption: disabled
NSRP authentication: disabled
device based nsrp monitoring thresholD. 255, weighted sum: 0, not failed
device based nsrp monitor interfacE. ethernet2/1(weight 255, UP) ethernet2/3(weight 255, UP) ethernet2/4(weight 255, UP) ethernet2/5(weight 255, UP)
ethernet2/2(weight 255, UP)
device based nsrp monitor zonE.
device based nsrp track ip: (weight: 255, disabled)
number of gratuitous arps: 4 (default)
config synC. enabled
track ip: disabled

A. This cluster is configured as an active/active cluster.
B. RTO sync is enabled.
C. No secondary path is configured.
D. master-always-exists is enabled.
E. Only one interface is used for both the control and data links.

Correct Answer: BCD

QUESTION 50
Referring to the exhibit, both clustered devices are in a master state.
What is the cause of this situation?

NSPROD1(M)-> get nsrp ha-link
total_ha_port = 2
probe on ha-link is disabled
unused channel: ethernet8 (ifnum: 11) maC. 0010db1d1e8b statE. down unused channel: ethernet7 (ifnum: 10) maC. 0010db1d1e8a statE. down ha control link not available
ha data link not available
ha secondary path link not available

A. The cluster is not configured for NSRP.
B. The cluster is in the process of failing over from the primary node to the secondary node.
C. Probes on the HA links have been disabled, causing the HA links to go down.
D. The control and the data link is down.

Correct Answer: D

QUESTION 51
A host in the untrust zone sends 1000 SYN packets in a single second to a host in your trust zone destined for port 80.

Referring to the exhibit, which statement describes the behavior of the ScreenOS device?

```
ssg5-> get conf | include syn
set zone untrust screen syn-flood attack-threshold 625
set zone untrust screen syn-flood alarm-threshold 250
set zone untrust screen syn-flood timeout 20
set zone untrust screen syn-flood queue-size 1000
set zone untrust screen syn-flood
set flow syn-proxy syn-cookie
```

A. It will maintain this state for all 1000 connection attempts.
B. It will begin to drop the SYN packets.
C. It will block further connection attempts from this host for 20 seconds.
D. It will reply with SYN-ACK packets.

Correct Answer: D

QUESTION 52
Given the output shown in the exhibit, which command would you use to view the number of attacks that have been blocked by the Screen options on the Untrust zone?

```
nsisg2000-> get int

A - Active, I - Inactive, U - Up, D - Down, R - Ready

H - IPv6 Host Mode, O - IPv6 Router Mode
Interfaces in vsys Root:
Name           IP Address                Zone        MAC/INT-ID      VLAN State VSD Vsys
mgt            192.168.1.1/24            MGT         0010.dbc5.f200    -   U    -   Root
eth2/1         10.0.0.1/24               Untrust     0010.dbc5.f215    -   U    -   Root
eth2/2         192.168.2.1/24            Trust       0010.dbc5.f216    -   U    -   Root
eth3/1         10.0.5.1/24               Untrust     0010.dbc5.f21d    -   U    -   Root
eth3/2         0.0.0.0/0                 Null        0010.dbc5.f21e    -   U    -   Root
vlan1          0.0.0.0/0                 VLAN        0010.dbc5.f20f    1   D    -   Root
null           0.0.0.0/0                 Null        N/A               -   U    0   Root
```

A. ssg5-> get counter screen interface ethernet2/1
B. ssg5-> get zone Untrust screen
C. ssg5-> get counter screen zone Untrust
D. ssg5-> get counter statistics interface ethernet2/1

Correct Answer: C

QUESTION 53
Based on the output shown in the exhibit, in which log were these events displayed?

Date Time Module Level Type Description

2012-11-30 12:49:41 system warn 00528 SSH: Password authentication failed
for admin user 'firewall-user' at host
10.210.62.67.
2012-11-30 12:49:41 system warn 00518 ADM: Local admin authentication

failed
for login name firewall-user: invalid
login name
2012-11-30 12:49:28 system info 00536 IKE 66.129.232.26 Phase 1:
Retransmission limit has been reached.
2012-11-30 12:42:23 system notif 00531 The system clock was updated from
primary NTP server type 209.244.0.5
with an adjustment of 234 ms.
Authentication was None. Update mode
was Automatic

A. event
B. self
C. login
D. traffic

Correct Answer: A

QUESTION 54
Referring to the exhibit, what does this output show?

```
ns5gt-> get license-key
 ...
Sessions:            2064 sessions
Capacity:            unlimited number of users
NSRP:                Disable
VPN tunnels:         10 tunnels
Vsys:                None
Vrouters:            3 virtual routers
Zones:               6 zones
VLANs:               10 vlans
Drp:                 Enable
Deep Inspection:     Disable
Deep Inspection Database Expire Date: Disable
Signature pack:      N/A
IDP:                 Disable
AV:                  Disable(0)
Anti-Spam:           Disable(0)
Url Filtering:       Disable

Update server url: nextwave.netscreen.com/key_retrieval
License key auto update : Disabled
Auto update interval : 0 days
```

A. the number of supported physical interfaces on the device
B. the number of supported route tables on the device

C. the number of supported VRs on the device
D. the amount of system memory on the device

Correct Answer: C

QUESTION 55
Which ScreenOS security feature helps protect against port scans and denial of service attacks?

A. session-based stateful firewall
B. IPsec VPNs
C. security policies
D. Screen options

Correct Answer: D

QUESTION 56
What is the initial default username and password for all ScreenOS devices?

A. administrator/password
B. root/password
C. netscreen/netscreen
D. admin/netscreen1

Correct Answer: C

QUESTION 57
What is a virtual system?

A. a mechanism to logically partition a single ScreenOS device into multiple logical devices
B. a collection of subnets and interfaces sharing identical security requirements
C. a method of providing a secure connection across a network
D. a tool to protect against DoS attacks

Correct Answer: A

QUESTION 58
What is a zone?

A. a set of rules that controls traffic from a specified source to a specified destination using a specified service
B. a collection of subnets and interfaces sharing identical security requirements
C. a method of providing a secure connection across a network
D. a tool to protect against DoS attacks

Correct Answer: B

QUESTION 59
What is the function of NAT?

A. It performs Layer 3 routing.
B. It evaluates and redirects matching traffic into secure tunnels.
C. It provides translation between IP addresses.
D. It performs Layer 2 switching.

Correct Answer: C

QUESTION 60
On a ScreenOS device, which word appears at the beginning of configuration commands?

A. set
B. configure
C. enable
D. commit

Correct Answer: A

QUESTION 61
Which action does a ScreenOS device perform first when processing a packet?

A. It checks for an existing session.
B. It checks for attacks in the payload.
C. It performs a route lookup.
D. It performs a policy lookup.

Correct Answer: A

QUESTION 62
On a ScreenOS device, which three processes does the task CPU handle? (Choose three.)

A. policy evaluation
B. traffic logging
C. session table clean-up
D. management services
E. broadcast packet processing

Correct Answer: BCD

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

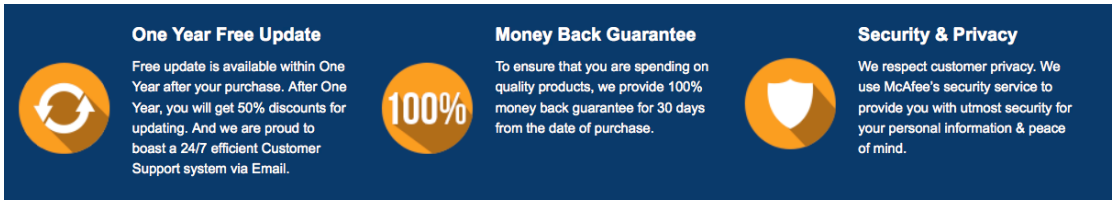
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

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

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions