Juniper

Exam JN0-696

Security Support, Professional (JNCSP-SEC)

Version: 9.0

[Total Questions: 71]

Question No : 1

-- Exhibit -user@host> show security flow session

...

Session ID. 41, Policy name: allow/5, Timeout: 20, Valid

In: 172.168.66.143/43886 --> 192.168.100.1/5000;tcp, If: ge-0/0/1.0, Pkts: 1, Bytes: 60 Out: 10.100.1.100/5555 --> 172.168.66.143/43886;tcp, If: ge-0/0/2.0, Pkts: 0, Bytes: 0

user@host> show configuration

...

security { nat { destination { pool server {

address 10.100.1.100/32 port 5555;

}

rule-set rule1 { from zone UNTRUST;

rule 1 { match {

destination-address 192.168.100.1/32;

destination-port 5000;

} then {

destination-nat pool server;

}

}

}

}

proxy-arp {

interface ge-0/0/1.0 { address {

192.168.100.1/32;

}

}

```
}
} policies {
from-zone UNTRUST to-zone TRUST {
policy allow {
match { source-address any; destination-address any;
application [ junos-ping tcp-5000 ];
} then { permit;
}
}
}
}
zones {
security-zone TRUST { interfaces { ge-0/0/2.0 {
host-inbound-traffic {
protocols { all;
}
}
}
}
}
security-zone UNTRUST {
interfaces { ge-0/0/1.0 { host-inbound-traffic { system-services {
ping;
}
}
}
```

}

}

}

} applications { application tcp-5000 { protocol tcp;

destination-port 5000;

}

}

-- Exhibit --

Click the Exhibit button.

Your customer is attempting to reach your new server that should be accessible publicly using 192.168.100.100 on TCP port 5000, and internally using 10.100.100.1 on TCP port 5555. You notice a session forms when they attempt to access the server, but they are unable to reach the server.

Referring to the exhibit, what will resolve this problem?

A. There must be a TRUST-to-UNTRUST security policy to allow return traffic.
B. The NAT pool server address must be changed to 10.100.100.1/32.
C. The NAT pool server port must be changed to 5000.
D. The NAT rule set rule1 must match on address 172.168.66.143.

Answer: B

Question No : 2

Click the Exhibit button.

```
user@srx> show chassis cluster status
Cluster ID: 1
Node      Priority  Status         Preempt   Manual failover

Redundancy group: 0, Failover count: 1
node0     100       primary        no        no
node1     0         lost           no        no

Redundancy group: 1, Failover count: 1
node0     100       primary        no        no
node1     0         lost           no        no
```

You recently configured a chassis cluster between two branch SRX Series devices and realize that the cluster is not functional, with node device status lost.

Referring to the exhibit, which two actions will correct this problem? (Choose two.)

A. Confirm both devices are synchronized with the local NTP.
B. Confirm that the software on both devices is the same Junos OS version.
C. Confirm both devices are running with the same security policies.
D. Confirm that the hardware on both devices is the same.

Answer: B,D

Explanation:

Chassis Cluster prerequisites include:
B: The SOFTWARE on both standalone devices must be the same Junos OS version.
Verify using this command on both devices:
root> show version
Model: srx220h
JUNOS Software Release [11.4R7.5]
D: Confirm that the HARDWARE on both devices is the same.
Verify using this command on both devices: root@srx220> show chassis hardware detail
References:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB21312&actp=search

Question No : 3

Click the Exhibit button.

```
set security policies from-zone trust to-zone trust policy
default-permit match source-address any
set security policies from-zone trust to-zone trust policy
default-permit match destination-address any
set security policies from-zone trust to-zone trust policy
default-permit match application any
set security policies from-zone trust to-zone trust policy
default-permit then permit
```

A customer created a security policy and is not receiving any logs from permitted sessions, you are asked to obtain the logs for the customer.

Which parameter must you add to the configuration shown in the exhibit to accomplish this task?

A. set system syslog file traffic-log any any
B. set default-permit then log session-close
C. set default-permit then count
D. set system syslog file traffic-log match “traffic_session”.

Answer: A

Explanation:

To send security policy logs to a file named traffic-log on the SRX Series device: user@host# set system syslog file traffic-log any any user@host# set system syslog file traffic-log match "RT_FLOW_SESSION"
In the example above, traffic log messages are sent to a separate log file named traffic-log. The severity level is set to any so that the traffic log messages are captured. Only log messages that match RT_FLOW_SESSION, which identifies traffic log messages, are sent to the traffic-log file.
References:
http://kb.juniper.net/InfoCenter/index?page=content&id=KB16509&actp=search

Question No : 4

Click the Exhibit button.

```
[edit security nat destination]
user@srx# show
pool LOCAL-POOL-A {
     address 10.5.0.5/32;
}
rule-set 1 {
     from zone untrust;
     rule A {
          match {
               destination-address 200.10.10.1/32;
          }
          then {
               destination-nat {
                    off;
                    }
               }
          }
     }
}
```

A customer is using a destination NAT to a remote webserver, but the configuration is not working.

Referring to the exhibit, which configuration changes will resolve this problem?

```
A.
[edit security nat destination rule-set 1 rule A]
user@srx# show
        match {
                destination-address 200.10.10.1/32;
                destination-port {
                        80;
                }
        }
        then {
                destination-nat {
                        pool {
                                LOCAL-POOL-A;
                                }
                        }
                }

B.
[edit security nat destination rule-set 1 rule A]
user@srx# show
        match {
                destination-address 200.10.10.1/32;
                destination-port {
                        80;
                }
        }
        then {
                destination-nat {
                        pool ~
                }
        }

C.
[edit security nat destination rule-set 1]
user@srx# show
        match {
                source-address 0.0.0.0/0;
                destination-address 200.10.10.1/32;
        }
        then {
                destination-nat {
                        pool {
                                LOCAL-POOL-A; ~
                        }
                }
        }

D.
[edit security nat destination]
user@srx# show
pool LOCAL-POOL-A {
        address 10.5.0.5/32 port 8080;
}
rule-set 1 {
        from zone untrust;
        rule A {
                match {
                        source-address 0.0.0.0/0;
                        destination-address 200.10.10.1/32;
                        destination-port {
                                80;
                }
        }
}
```

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

Example of working configuration: user@host# show security nat
destination { pool dst-nat-pool-1 {
address 192.168.1.200/32;
}
rule-set rs1 {
from interface ge-0/0/0.0;
rule r1 { match {
destination-address 1.1.1.200/32;
} then {
destination-nat pool dst-nat-pool-1;
}
}
}
}

References:
http://www.juniper.net/documentation/en_US/junos12.1x46/topics/example/nat-securitydestination-single-address-translation-configuring.html

Question No : 5

-- Exhibit --

user@R1> show security ike security-associations user@R1> show security zones

Security zone: trust

Send reset for non-SYN session TCP packets: Off

Policy configurable: Yes Interfaces bounD. 3 Interfaces: ge-0/0/0.0 ge-0/0/6.0 lo0.0

Security zone: untrust

Send reset for non-SYN session TCP packets: Off

Policy configurable: Yes Interfaces bounD. 1 Interfaces: ge-0/0/1.0

Security zone: junos-host

Send reset for non-SYN session TCP packets: Off

Policy configurable: Yes Interfaces bounD. 0 Interfaces:

user@R1> show interfaces st0

Physical interface: st0, Enabled, Physical link is Up

Interface index: 130, SNMP ifIndex: 503

Type: Secure-Tunnel, Link-level type: Secure-Tunnel, MTU: 9192

Device flags : Present Running

Interface flags: Point-To-Point

Input rate : 0 bps (0 pps)

Output rate : 0 bps (0 pps)

Logical interface st0.0 (Index 72) (SNMP ifIndex 546)

Flags: Link-Layer-Down Point-To-Point SNMP-Traps

Encapsulation: Secure-Tunnel

Input packets : 3

Output packets: 3

Security: Zone: Null

Protocol inet, MTU: 9192

Flags: Sendbcast-pkt-to-re

Addresses, Flags: Dest-route-down Is-Preferred Is-Primary

Destination: 172.19.0.0/30, Local: 172.19.0.1

user@R1> show interfaces ge-0/0/1

Physical interface: ge-0/0/1, Enabled, Physical link is Up

Interface index: 135, SNMP ifIndex: 508

Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, SpeeD. 1000mbps,

BPDU Error: None, MAC-REWRITE Error: None, Loopback: Disabled,

Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,

Remote fault: Online

Device flags : Present Running

Interface flags: SNMP-Traps Internal: 0x0

Link flags : None

CoS queues : 8 supported, 8 maximum usable queues

Current address: b0:c6:9a:73:27:81, Hardware address: b0:c6:9a:73:27:81

Last flapped : 2013-06-12 15:22:48 UTC (00:59:41 ago)

Input rate : 0 bps (0 pps)

Output rate : 0 bps (0 pps)

Active alarms : None

Active defects : None

Interface transmit statistics: Disabled

Logical interface ge-0/0/1.0 (Index 71) (SNMP ifIndex 541)

Flags: SNMP-Traps 0x0 Encapsulation: ENET2

Input packets : 40

Output packets: 27

Security: Zone: untrust

Allowed host-inbound traffic : ping

Protocol inet, MTU: 1500

Flags: Sendbcast-pkt-to-re

Addresses, Flags: Is-Preferred Is-Primary

Destination: 184.0.15.0/30, Local: 184.0.15.1, Broadcast: 184.0.15.3

user@R1> show log ipsec-trace | match "500|drop"

Jun 12 16:32:10 16:32:10.680034:CID-0:RT:ageout 71,184.0.15.2/500->184.0.15.1/500,17, (0/0) Jun 12 16:32:51 16:32:51.874191:CID-0:RT:184.0.15.2/500->184.0.15.1/500;17> :

Jun 12 16:32:51 16:32:51.874191:CID-0:RT: ge-0/0/1.0:184.0.15.2/500->184.0.15.1/500,

udp

Jun 12 16:32:51 16:32:51.874191:CID-0:RT: find flow: table 0x4f160b38, hash 8769(0xffff), sa 184.0.15.2, da

184.0.15.1, sp 500, dp 500, proto 17, tok 8

Jun 12 16:32:51 16:32:51.874191:CID-0:RT:pak_for_self : proto 17, dst port 500, action 0x0

Jun 12 16:32:51 16:32:51.874191:CID-0:RT: flow_first_in_dst_nat: in 0/1.0>, out A> dst_adr 184.0.15.1, sp 500, dp 500

Jun 12 16:32:51 16:32:51.874555:CID-0:RT: packet droppeD. for self but not interested

Jun 12 16:32:51 16:32:51.874555:CID-0:RT: packet dropped, packet droppeD. for self but not interested. Jun 12 16:32:54 16:32:54.680399:CID-0:RT:ageout 71,184.0.15.2/500->184.0.15.1/500,17, (0/0) Jun 12 16:32:56 16:32:56.888094:CID-0:RT:184.0.15.2/500->184.0.15.1/500;17> :

Jun 12 16:32:56 16:32:56.888094:CID-0:RT: ge-0/0/1.0:184.0.15.2/500->184.0.15.1/500, udp

Jun 12 16:32:56 16:32:56.888094:CID-0:RT: find flow: table 0x4f160b38, hash 8769(0xffff), sa 184.0.15.2, da

184.0.15.1, sp 500, dp 500, proto 17, tok 8

Jun 12 16:32:56 16:32:56.888094:CID-0:RT:pak_for_self : proto 17, dst port 500, action 0x0

Jun 12 16:32:56 16:32:56.888094:CID-0:RT: flow_first_in_dst_nat: in 0/1.0>, out A> dst_adr 184.0.15.1, sp 500, dp 500

Jun 12 16:32:56 16:32:56.888094:CID-0:RT: packet droppeD. for self but not interested

Jun 12 16:32:56 16:32:56.888094:CID-0:RT: packet dropped, packet droppeD. for self but not interested. Jun 12 16:33:00 16:33:00.680794:CID-0:RT:ageout 71,184.0.15.2/500->184.0.15.1/500,17, (0/0) Jun 12 16:33:07 16:33:06.902220:CID-0:RT:184.0.15.2/500->184.0.15.1/500;17> :

Jun 12 16:33:07 16:33:06.902220:CID-0:RT: ge-0/0/1.0:184.0.15.2/500->184.0.15.1/500, udp

Jun 12 16:33:07 16:33:06.902220:CID-0:RT: find flow: table 0x4f160b38, hash 8769(0xffff), sa 184.0.15.2, da 184.0.15.1, sp 500, dp 500, proto 17, tok 8

Jun 12 16:33:07 16:33:06.902220:CID-0:RT:pak_for_self : proto 17, dst port 500, action 0x0

Jun 12 16:33:07 16:33:06.902220:CID-0:RT: flow_first_in_dst_nat: in 0/1.0>, out A> dst_adr 184.0.15.1, sp 500, dp 500

Jun 12 16:33:07 16:33:06.902220:CID-0:RT: packet droppeD. for self but not interested

Jun 12 16:33:07 16:33:06.902220:CID-0:RT: packet dropped, packet droppeD. for self but not interested. -- Exhibit --

Click the Exhibit button.

You are asked to troubleshoot a new IPsec tunnel that is not establishing between R1 and R2. The remote team has verified that R2's configuration is correct.

Referring to the exhibit, which two actions are required to resolve the problem? (Choose two.)

A. Add the st0.0 interface to a security zone.
B. Change the st0.0 interface MTU to 1400.
C. Enable IKE for host inbound traffic in the untrust zone.
D. Enable IKE for host inbound traffic in the trust zone.

Answer: A,C

Question No : 6

Click the Exhibit button.

```
[edit security policies from-zone trust to-zone untrust]
user@srx# show
policy user {
     match {
          source-address 192.168.1.1-2;
          destination-address any;
          application any;
     }
     then {
          permit;
     }
}
user@srx# commit
[edit security policies from-zone trust to-zone untrust]
     'policy user'
       Source address or address_set (192.168.1.1-2) not found.
error: configuration check-out failed
```

A customer wants to commit a configuration but receives the error shown in the exhibit.

A.
```
set security zones security-zone trust address-book address add1 192.168.1.1/32
set security zones security-zone trust address-book address add2 192.168.1.2/32
set security zones security-zone trust address-book address-set book1 address add1
set security zones security-zone trust address-book address-set book1 address add2
set security policies from-zone trust to-zone untrust policy user match source-addre
```

B.
```
set security policies from-zone trust to-zone untrust policy user match source-addre
[192.168.1.1/32 192.168.1.2/32]
```

C.
```
set security zones security-zone trust address-book address add1 192.168.1.1-2
set security zones security-zone trust address-book address-set book1 address add1
set security policies from-zone trust to-zone untrust policy user match source-addre
```

D.
```
set security zones security-zone trust address-book address-set book1 address 192.16
set security zones security-zone trust address-book address-set book1 address 192.16
set security policies from-zone trust to-zone untrust policy user match source-addre
```

What would solve the problem?

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

The Source address or address_set not found error message indicates that we need to create addressbook entries for
192.168.1.1 and 192.168.1.2.

Question No : 7

You recently installed a new webserver which resides in the DMZ zone of an SRX Series device. However, the server is not accessible from any host in the Untrust zone.

Which two statements are true? (Choose two.)

A. A security policy must be configured to allow traffic from the Untrust zone destined to the DMZ zone.
B. The webserver and the SRX Series device must be configured to use the same NTP server.

C. The webserver's IP address must be represented in an address book entry on the SRX Series device.
D. The SRX Series device must be configured to allow SSH as host-inbound-traffic.

Answer: A,C

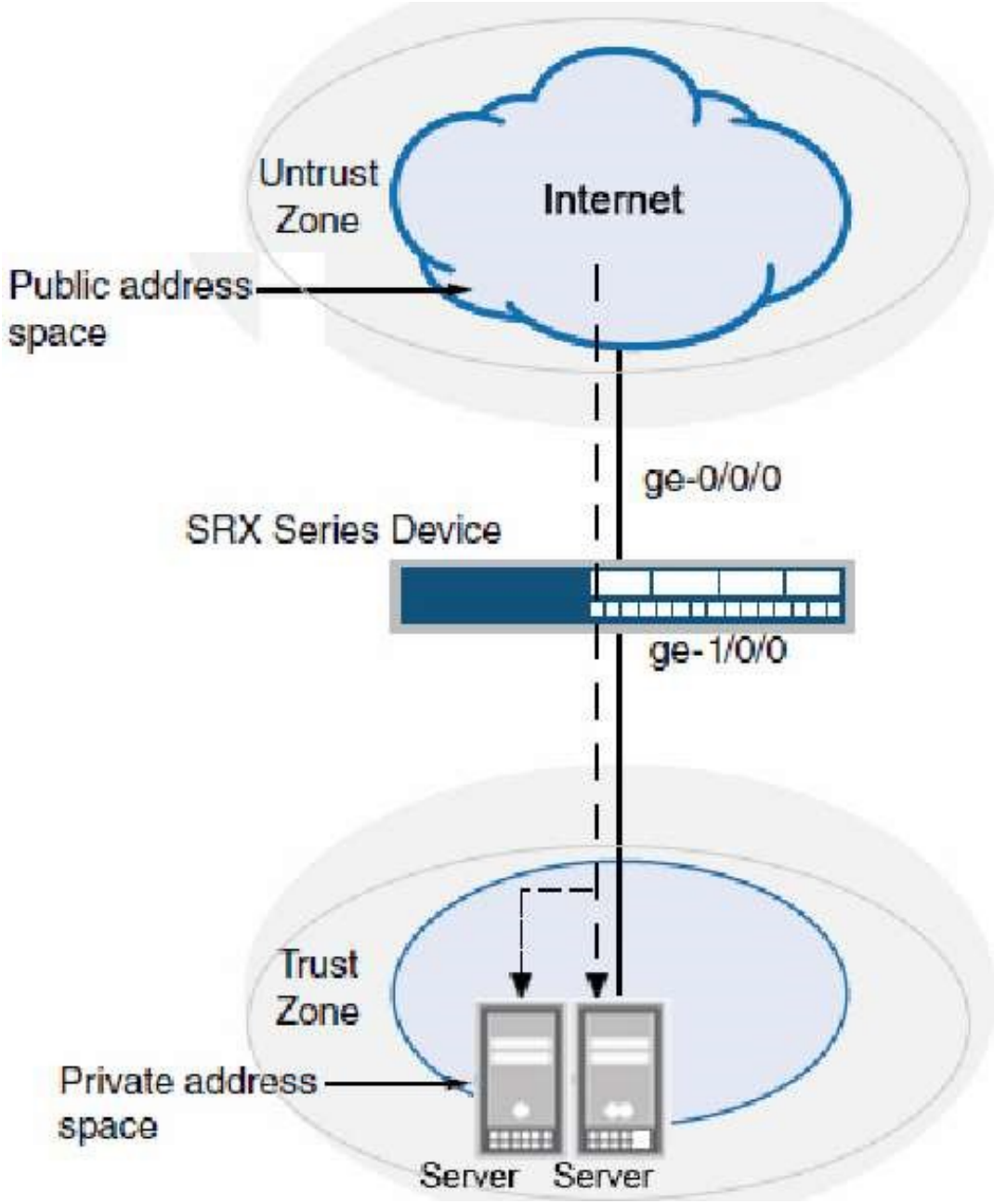
Explanation:

C: Example: set security zones security-zone dmz address-book address webserver 172.16.1.250/24 - Creates an address book entry for the webserver
References:
http://www.juniper.net/documentation/en_US/junos12.1x47/topics/example/security-srx-device-natconfiguring.html http://www.juniper.net/us/en/local/pdf/app-notes/3500153-en.pdf

Question No : 8

Click the exhibit button.

```
set security nat destination pool Web-server-1 address
10.10.10.10/32
set security nat destination pool Web-server-1 address port 80
set security nat destination pool Web-server-2 address
10.10.10.20/32
set security nat destination pool Web-server-2 address port 8000
set security nat destination rule-set rs1 from zone untrust
set security nat destination rule-set rs1 rule r1 match
destination-address 190.133.117.184/32
set security nat destination rule-set rs1 rule r1 match
destination-port 80
set security nat destination rule-set rs1 rule r1 then
destination-nat pool Web-server-1
set security nat destination rule-set rs1 rule r2 match
destination-address 190.133.117.184/32
set security nat destination rule-set rs1 rule r2 match
destination-port 8000
set security nat destination rule-set rs1 rule r2 then
destination-nat pool Web-server-2
```



You recently installed two new internal webservers. You configure destination NAT on your SRX Series device so that external users will have access to internal Web resources. However, the external users reported that they still do not have access to the server.

Referring to the exhibit, what should you do to solve the problem?

A. Configure proxy ARP for the address 190.133.117.184/32.
B. Contact your ISP since the packets are not reaching the SRX Series device.
C. Configure 190.133.117.184/32 under a security zone.
D. Configure a different IP address for the internal servers.

Answer: C

Explanation:

An interface for a security zone can be thought of as a doorway through which TCP/IP traffic can pass between that zone and any other zone.
Through the policies you define, you can permit traffic between zones to flow in one direction or in both. With the routes that you define, you specify the interfaces that traffic from one zone to another must use
Note: A security zone is a collection of one or more network segments requiring the regulation of inbound and outbound traffic through policies. Security zones are logical entities to which one or more interfaces are bound.
References:
http://www.juniper.net/techpubs/en_US/junos12.1x44/information-products/pathway-pages/security/securitybasic-zone-interface.pdf

Question No : 9

Click the Exhibit button.

```
user@srx# set forwarding-options helpers bootp description "Global DHCP relay
service"
user@srx# set forwarding-options helpers bootp server 192.18.24.38
user@srx# set forwarding-options helpers bootp maximum-hop-count 4
user@srx# set forwarding-options helpers bootp interface ge-0/0/7.0
user@srx# set security zones security-zone untrust address-book address DHCP-
server 192.168.24.38
user@srx# set security policies from-zone trust to-zone untrust policy DHCP-
request match source-address any
user@srx# set security policies from-zone trust to-zone untrust policy DHCP-
request match destination-address DHCP-server
user@srx# set security policies from-zone trust to-zone untrust policy DHCP-
request match application any
user@srx# set security policies from-zone trust to-zone untrust policy DHCP-
request then permit
user@srx# set security policies from-zone untrust to-zone trust policy DHCP-
reply match source-address DHCP-server
user@srx# set security policies from-zone untrust to-zone trust policy DHCP-
reply match destination-address any
user@srx# set security policies from-zone untrust to-zone trust policy DHCP-
reply match application any
user@srx# set security policies from-zone untrust to-zone trust policy DHCP-
reply then permit
```

A customer configured DHCP relay. After committing the configuration, the DHCP server does not provide addresses and you suspect that a configuration is missing. The server is connected to ge-0/0/8 and the hosts are connected to ge-0/0/7 through a switch. The server IP address is 192.18.24.38.

Referring to the exhibit, which two commands would be used to solve the problem? (Choose two.)

A. set security zones security-zone trust interfaces ge-0/0/7 host-inbound-traffic system-

services dhcp
B. set security policies from-zone untrust to-zone trust policy DHCP-reply match destination-address 192.18.24.38
C. set security policies from-zone trust to-zone untrust policy DHCP-request match source-address 192.18.24.38
D. set security zones security-zone untrust interfaces ge-0/0/8 host-inboundtraffic system-services dhcp

Answer: A,C
Explanation:

SRX Getting Started - Configure Global DHCP Relay Service
A: Specify DHCP as an allowed inbound service for each interface that is associated with DHCP. In the following example, DHCP is configured as an inbound service for ge-0/0/7.
user@host# set security zones security-zone trust interfaces ge-0/0/7 host-inbound-traffic system-services dhcp
C: Make sure that you have a security policy that allows the session from the DHCP server to the DHCP client apart for the policy from trust to untrust.
Example:
user@host# set security policies from-zone trust to-zone untrust policy DHCP-request match destinationaddress DHCP-server
References:
https://kb.juniper.net/InfoCenter/index?page=content&id=KB15755&pmv=print&actp=LIST

Question No : 10

You are troubleshooting a problem on your Junos device where the antispam SBL server is no longer filtering known spam hosts. You notice that local list antispam filtering is still working for known spam hosts.

What would cause this problem?

A. You have configured the sbl-default-server parameter in the antispam feature profile.
B. DNS has stopped working on your Junos device.
C. The antispam license has expired on your Junos device.
D. The default spam-action parameter has been set to permit.

Answer: C
Explanation:

When it stops working remotely but still works locally it is normally due to the license

expiring unless something else has changed in your configuration.
References:
http://www.juniper.net/documentation/en_US/junos12.1/topics/concept/utm-antispam-filter-server-basedunderstanding.html

Question No : 11

Click the Exhibit button.

```
[edit security zones]
user@srx# show
security-zone trust {
     tcp-rst;
     host-inbound-traffic {
          system-services {
               all;
          }
          protocols {
               all;
          }
     }
     interfaces {
          lo0.0;
          ge-0/0/1.0;
     }
}
security-zone untrust {
     screen untrust-screen;
     interfaces {
          ge-0/0/0.0 {
               host-inbound-traffic {
                    system-services {
                         dhcp;
                         http;
                         https;
                         telnet;
                    }
               }
          }
     }
}
```

A customer has a problem connecting to an SRX Series device from the untrust zone using SSH only.

Referring to the exhibit, which action will solve the problem?

A. Configure the ssh parameter under the [edit security zones security-zone trust interfaces ge-0/0/1.0 host inbound-traffic protocols] hierarchy.
B. Configure the ssh parameter under the [edit security zones security-zone untrust hostinbound-traffic system-services] hierarchy.
C. Configure the ssh parameter under the [edit security zones security-zone untrust hostinbound-traffic protocols] hierarchy.
D. Configure the ssh parameter under the [edit security zones security-zone trust hostinbound-traffic system-services] hierarchy.

Answer: B

Explanation:

Assume that inbound ssh, ftp, and ping traffic should be permitted from the untrusted zone. Then you should do the following:
[edit security zones]
root# set security zone untrust host-inbound-traffic ssh root# set security zone untrust host-inbound-traffic ftp root# set security zone untrust host-inbound-traffic ping
Note: For SRX Series branch devices, a factory default security policy is provided that:
Allows all traffic from the trust zone to the untrust zone.
Allows all traffic between trusted zones, that is from the trust zone to intrazone trusted zones. Denies all traffic from the untrust zone to the trust zone.
References: http://www.dummies.com/how-to/content/how-to-configure-srx-security-zones-with-junos.html
http://www.juniper.net/documentation/en_US/junos12.3x48/topics/concept/security-srx-device-zone-and-policyunderstanding.html

Question No : 12

You want to allow remote users using PCs running Windows 7 to access the network using an IPsec VPN. You implement a route-based hub-and-spoke VPN; however, users report that they are not able to access the network.

What is causing this problem?

A. The remote clients do not have proper licensing.
B. Hub-and-spoke VPNs cannot be route-based; they must be policy-based.
C. The remote clients' OS is not supported.
D. Hub-and-spoke VPNs do not support remote client access; a dynamic VPN must be implemented instead.

Answer: D

Question No : 13

You have deployed AppID on your SRX Series device. You want to block all HTTP connections. However, there is a packet-monitoring device that shows the SRX Series device is still allowing some packets through to the webservers on TCP port 80.

In this scenario, which statement is correct?

A. Traffic is hitting the default fall-back option.
B. The packet-monitoring device is allowing packets to TCP port 80.
C. After deploying AppID, this is a normal behavior.
D. There are new sessions matching the webservers on TCP port 80.

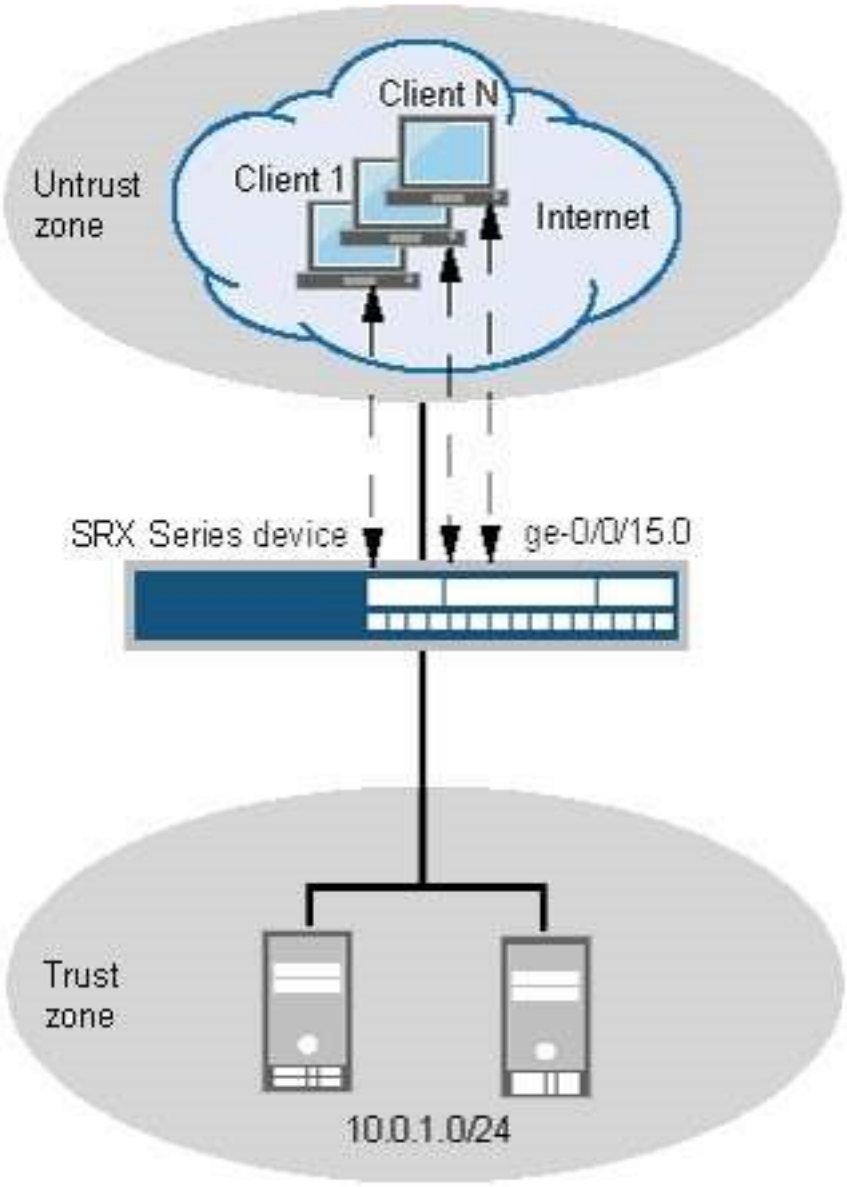
Answer: C

Explanation:

Note: The APPID (application identification) feature is a Junos OS feature that identifies applications as constituents of application groups in TCP/UDP/ICMP traffic.
References: http://www.juniper.net/techpubs/en_US/junos-mobility12.1/topics/concept/pcef-app-idoverview.html

Question No : 14

Click the Exhibit button.




```
set access profile dyn-vpn-access-profile client client1
firewall-user password "$9$uY4o0EyMWxclwgX7"
set access profile dyn-vpn-access-profile client client2
firewall-user password "$9$neNM9CuBihyrv5Q39"
set access profile dyn-vpn-access-profile address-assignment
pool dyn-vpn-address-pool
set access address-assignment pool dyn-vpn-address-pool family
inet network 10.0.1.0/24
set access address-assignment pool dyn-vpn-address-pool family
inet xauth-attributes primary-dns 4.2.2.2/32
set access firewall-authentication web-authentication default-
profle dyn-vpn-access-profile
```

A customer has requested that you set up a dynamic VPN to allow users to reach the internal network. After running the configuration shown in the exhibit, users are sometimes unable to connect to the network. They cannot ping other IP addresses and they are

getting IP conflicts within the network.

What must you change in the configuration to solve this problem?

A. The dyn-vpn-address-pool network address needs to be an address book.
B. The configuration is missing a secondary DNS.
C. The dyn-vpn-address-pool network address needs to be configured on a separate subnet.
D. The configuration needs to be applied to a different interface.

Answer: C
Explanation:

References:
http://www.juniper.net/documentation/en_US/junos12.3x48/topics/example/vpn-security-dynamic-exampleconfiguring.html

Question No : 15

Click the exhibit button.

```
May 19 13:01:33 :500 (Responder) -> 172.16.32.5:500 { 15276b72
6656c3b6 -29675811
96758116 [1] / 0x9828a32e } QM; Invalid protocol_id = O
May 19 13:01:34 Received authenticated notification payload
unknown from local:192.168.20.10
remote:172.16.32.5 IKEv1 for P1 SA 3075335
May 19 13:01:34 iked_pm_ike_spd_notify_receiveD. Negotiation is
already failed. Reason: TS
unacceptable.
May 19 13:01:34 QM notification '(null)' (40001) (size 8 bytes)
from 172.16.32.5 for protocol
Reserved spi[0…3]=0f f0 ce d3
May 19 13:01:34 ike_st_i_private: Start
May 19 13:01:34 ike_st_o_qm_hash_2: Start
May 19 13:01:34 ike_st_o_qm_sa_values: Start
May 19 13:01:34 :500 (Responder) -> 172.16.32.5:500 { 15276b72
6656c3b6 -29675811
6758116 [1] / 0x9828a32e } QM; Error = No proposal chosen (14)
```

Your customer has indicated that their VPN is down.

Referring to the exhibit, what is the problem? A. The IKE IDs are mismatched.

A. The proxy IDs are mismatched.
B. The IKE Phase 2 proposals are mismatched.

C. The IKE Phase 1 proposals are mismatched.

Answer: B

Explanation:

Example of IKE proxy-id mismatch (see line 11 onwards):
1 [Apr 2 10:57:34]SA-CFG lookup for Phase 2 failed for local:172.16.123.2, remote:172.16.123.1 IKEv1
2. [Apr 2 10:57:34]ikev2_fb_spd_select_qm_sa_cb: IKEv2 SA select failed with error TS unacceptable 3. [Apr 2 10:57:34]ikev2_fb_spd_select_qm_sa_cb: SA selection failed, no matching proposal (neg df6800)

11 [Apr 2 10:57:34]iked_pm_ike_spd_notify_received: Negotiation is already failed. Reason: TS unacceptable.
[Apr 2 10:57:34]QM notification `(null)' (40001) (size 8 bytes) from 172.16.123.1 for protocol Reserved spi[0...3] =eb 7b b2 b4
[Apr 2 10:57:34]ike_st_i_private: Start
[Apr 2 10:57:34]ike_st_o_qm_hash_2: Start
[Apr 2 10:57:34]ike_st_o_qm_sa_values: Start
Note: “A proxy-ID is used during phase 2 of Internet Key Exchange (IKE) Virtual Private Network (VPN) negotiations. Both ends of a VPN tunnel either have a proxy-ID manually configured (route-based VPN) or just use a combination of source IP, destination IP, and service in a tunnel policy. When phase 2 of IKE is negotiated, each end compares the configured local and remote proxy-ID with what is actually received. The configured proxy ID must match with what is received from the other device that is negotiating an IKE/IPsec tunnel.
References: http://www.twine-networks.com/blog/posts/5-troubleshooting-ipsec-log-messages

Question No : 16

Click the Exhibit button.

```
Jun 23 13:54:18 Unable to find ike gateway as remote peer:2.2.2.2 is not
recognized.
Jun 23 13:54:18 KMD_PM_P1_POLICY_LOOKUP_FAILURE: Policy lookup for Phase-1
[responder] failed for p1_local=ipv4(any:0,[0..3]=1.1.1.1)
p1_remote=ipv4(any:0,[0..3]=2.2.2.2)
Jun 23 13:54:18 1.1.1.1:500 (Responder) <-> 2.2.2.2:500 { 9c6c7b2e 5b6cc980 -
96757581 6758116 [-1] / 0x00000000 } IP; Error = No proposal chosen (14)
```

You are troubleshooting an IPsec VPN which is not establishing.

Which two issues would cause the message shown in the exhibit? (Choose two.)

A. mismatched peer ID type
B. Phase 2 proposal mismatch
C. mismatched pre-shared key
D. incorrect peer address

Answer: A,B

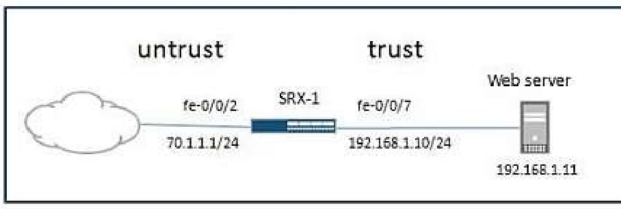
Question No : 17

Click the Exhibit button.

```
user@SRX-1# show security nat
destination {
    pool web {
        address 192.168.1.11/32 port 80;
    }
    rule-set http {
        from zone untrust;
        rule 1 {
            match {
                destination-address 70.1.1.1/32;
                destination-port 80;
            }
            then {
                destination-nat pool web;
            }
        }
    }
}

user@SRX-1# show security policies from-zone untrust to-zone trust
policy web-server-policy {
    match {
        source-address any;
        destination-address web-server;
        application junos-http;
    }
    then {
        permit;
    }
}

user@SRX-1# show security address-book global
address web-server 70.1.1.1/32;
```



Your company has a Web server in the trust zone. You configure a NAT rule to allow Internet users from the untrust zone to access this Web server. Internet users use the public IP address 70.1.1.1 to access this Web server, but they report that the server is not accessible.

Referring to the exhibit, which configuration change would resolve this problem?

A. set security nat proxy-arp interface fe-0/0/2 address 70.1.1.0/24

B. set security zones security-zone untrust host-inbound-traffic system-services http
C. set security nat destination rule-set http rule 1 match source-address 0.0.0.0/0
D. set security address-book global address web-server 192.168.1.11/32

Answer: D

Explanation:

DNAT is first, followed by Policy look-up.

Question No : 18

Click the Exhibit button.

```
{primary:node0}
user@srx> show chassis cluster interfaces
Control link 0 name: fxp1
Control link status: Up

Fabric interfaces:
     Name       Child-interface     Status
     fab0       ge-0/0/2            up
     fab0
     fab1       ge-9/0/2            up
     fab1
Fabric link status: Up

Redundant-ethernet Information:
     Name       Status              Redundancy-group
     reth0      Down                1
     reth1      Down                1
     reth2      Down                Not configured
     reth3      Down                Not configured

Interface Monitoring:
     Interface      Weight    Status    Redundancy-group
     ge-0/0/1       255       Down      1
     ge-9/0/1       255       Up        1
     ge-9/0/0       255       Down      1
     ge-0/0/0       255       Down      1

{primary:node0} user@srx> show chassis cluster status

Cluster ID: 3
     Node name Priority  Status    Preempt   Manual failover
Redundancy-group: 0, Failover count: 1
     node0     254       primary   no        no
     node1     2         secondary no        no
Redundancy-group: 1, Failover count: 1
     node0     254       primary   no        no
     node1     1         secondary no        no
```

You are implementing a high availability chassis cluster on an SRX Series device. You would like to manage both devices through the J-Web utility. However, when you try to log in to the second device using SSL HTTP, you receive a message from your Web browser indicating that the message has timed out.

Why you are receiving this message?

A. There is a firewall policy blocking traffic to the control plane.
B. HTTP is not configured as host inbound traffic.
C. The incoming traffic is not being allowed on the correct port.
D. The rdp daemon is on standby on the secondary device.

Answer: A

Question No : 19

-- Exhibit --

{primary:node0}

user@host> show configuration chassis | display inheritance cluster { redundancy-group 1 { node 0 priority 200; node 1 priority 100; interface-monitor { ge-0/0/12 weight 255; ge-5/0/12 weight 255;

}

}

}

-- Exhibit --

Click the Exhibit button.

A customer reports that their SRX failover is not working as expected. They expected node1 to become the primary node for the control plane when interface ge-0/0/12 failed. However, when ge-0/0/12 failed, node0 remained the primary node. They send you the output shown in the exhibit.

What is causing this problem?

A. The interface-monitor configuration should be applied to redundancy-group 0.
B. The redundancy-group configuration should include the preempt parameter.
C. The weight parameter applied to ge-5/0/12 is too high.
D. The weight parameter applied to ge-0/0/12 is too low.

Answer: A

Explanation:

Node 0 remains the master for the routing engine and therefore the “control plane”, because the configuration applies to RG1 not RG0. The data plane or the forwarding for RG1 would failover in this instance which might mean nothing for the customer.

Question No : 20

-- Exhibit --

[edit security utm] user@host# show custom-objects { url-pattern { blocklist {

value [http://badsite.com http://blocksite.com];

} acceptlist {

value http://juniper.net;

}

}

custom-url-category { blacklist { value blocklist;

} whitelist {

value acceptlist;

}

} }

feature-profile { web-filtering { url-whitelist whitelist; url-blacklist blacklist; type juniper-local; juniper-local { profile web-filter {

custom-block-message "Site is not allowed"; fallback-settings { default log-and-permit;

}

}

}

}

}

utm-policy utm1 { web-filtering {

http-profile web-filter;

}

}

-- Exhibit --

Click the Exhibit button.

You set up Web filtering to allow employees to only access your internal website. You notice that employees are still able to reach websites outside of the blacklists.

Referring the exhibit, which parameter must be changed?

A. You must define all sites you want to block using the mime-pattern parameter.
B. You must change the fallback-settings parameter to default block.
C. You must use integrated or redirect Web filtering instead of local list filtering.
D. You must define all sites you want to block using the protocol-command parameter.

Answer: C

Explanation:

Incorrect:
A, D: These are options for content filtering as opposed to web filtering. B: Fallback is for error conditions.

Question No : 21

-- Exhibit -user@host> show configuration security utm custom-objects { url-pattern { block-juniper {

value *.spammer.com;

}

}

custom-url-category { blacklist {

value block-juniper;

}

} }

feature-profile { anti-spam {

address-blacklist block-juniper; sbl {

profile myprofile { no-sbl-default-server;

spam-action block;

}

}

}

Microsoft Exams List

70-246 Dump PDF VCE	70-485 Dump PDF VCE	70-742 Dump PDF VCE	98-366 Dump PDF VCE
70-247 Dump PDF VCE	70-486 Dump PDF VCE	70-743 Dump PDF VCE	98-367 Dump PDF VCE
70-331 Dump PDF VCE	70-487 Dump PDF VCE	70-744 Dump PDF VCE	98-368 Dump PDF VCE
70-332 Dump PDF VCE	70-488 Dump PDF VCE	70-761 Dump PDF VCE	98-369 Dump PDF VCE
70-333 Dump PDF VCE	70-489 Dump PDF VCE	70-762 Dump PDF VCE	98-372 Dump PDF VCE
70-334 Dump PDF VCE	70-490 Dump PDF VCE	70-765 Dump PDF VCE	98-373 Dump PDF VCE
70-339 Dump PDF VCE	70-491 Dump PDF VCE	70-768 Dump PDF VCE	98-374 Dump PDF VCE
70-341 Dump PDF VCE	70-492 Dump PDF VCE	70-980 Dump PDF VCE	98-375 Dump PDF VCE
70-342 Dump PDF VCE	70-494 Dump PDF VCE	70-981 Dump PDF VCE	98-379 Dump PDF VCE
70-345 Dump PDF VCE	70-496 Dump PDF VCE	70-982 Dump PDF VCE	MB2-700 Dump PDF VCE
70-346 Dump PDF VCE	70-497 Dump PDF VCE	74-343 Dump PDF VCE	MB2-701 Dump PDF VCE
70-347 Dump PDF VCE	70-498 Dump PDF VCE	74-344 Dump PDF VCE	MB2-702 Dump PDF VCE
70-348 Dump PDF VCE	70-499 Dump PDF VCE	74-409 Dump PDF VCE	MB2-703 Dump PDF VCE
70-354 Dump PDF VCE	70-517 Dump PDF VCE	74-678 Dump PDF VCE	MB2-704 Dump PDF VCE
70-383 Dump PDF VCE	70-532 Dump PDF VCE	74-697 Dump PDF VCE	MB2-707 Dump PDF VCE
70-384 Dump PDF VCE	70-533 Dump PDF VCE	77-420 Dump PDF VCE	MB2-710 Dump PDF VCE
70-385 Dump PDF VCE	70-534 Dump PDF VCE	77-427 Dump PDF VCE	MB2-711 Dump PDF VCE
70-410 Dump PDF VCE	70-640 Dump PDF VCE	77-600 Dump PDF VCE	MB2-712 Dump PDF VCE
70-411 Dump PDF VCE	70-642 Dump PDF VCE	77-601 Dump PDF VCE	MB2-713 Dump PDF VCE
70-412 Dump PDF VCE	70-646 Dump PDF VCE	77-602 Dump PDF VCE	MB2-714 Dump PDF VCE
70-413 Dump PDF VCE	70-673 Dump PDF VCE	77-603 Dump PDF VCE	MB2-715 Dump PDF VCE
70-414 Dump PDF VCE	70-680 Dump PDF VCE	77-604 Dump PDF VCE	MB2-716 Dump PDF VCE
70-417 Dump PDF VCE	70-681 Dump PDF VCE	77-605 Dump PDF VCE	MB2-717 Dump PDF VCE
70-461 Dump PDF VCE	70-682 Dump PDF VCE	77-881 Dump PDF VCE	MB2-718 Dump PDF VCE
70-462 Dump PDF VCE	70-684 Dump PDF VCE	77-882 Dump PDF VCE	MB5-705 Dump PDF VCE
70-463 Dump PDF VCE	70-685 Dump PDF VCE	77-883 Dump PDF VCE	MB6-700 Dump PDF VCE
70-464 Dump PDF VCE	70-686 Dump PDF VCE	77-884 Dump PDF VCE	MB6-701 Dump PDF VCE
70-465 Dump PDF VCE	70-687 Dump PDF VCE	77-885 Dump PDF VCE	MB6-702 Dump PDF VCE
70-466 Dump PDF VCE	70-688 Dump PDF VCE	77-886 Dump PDF VCE	MB6-703 Dump PDF VCE
70-467 Dump PDF VCE	70-689 Dump PDF VCE	77-887 Dump PDF VCE	MB6-704 Dump PDF VCE
70-469 Dump PDF VCE	70-692 Dump PDF VCE	77-888 Dump PDF VCE	MB6-705 Dump PDF VCE
70-470 Dump PDF VCE	70-695 Dump PDF VCE	77-891 Dump PDF VCE	MB6-884 Dump PDF VCE
70-473 Dump PDF VCE	70-696 Dump PDF VCE	98-349 Dump PDF VCE	MB6-885 Dump PDF VCE
70-480 Dump PDF VCE	70-697 Dump PDF VCE	98-361 Dump PDF VCE	MB6-886 Dump PDF VCE
70-481 Dump PDF VCE	70-698 Dump PDF VCE	98-362 Dump PDF VCE	MB6-889 Dump PDF VCE
70-482 Dump PDF VCE	70-734 Dump PDF VCE	98-363 Dump PDF VCE	MB6-890 Dump PDF VCE
70-483 Dump PDF VCE	70-740 Dump PDF VCE	98-364 Dump PDF VCE	MB6-892 Dump PDF VCE
70-484 Dump PDF VCE	70-741 Dump PDF VCE	98-365 Dump PDF VCE	MB6-893 Dump PDF VCE

Cisco Exams List

010-151 Dump PDF VCE	350-018 Dump PDF VCE	642-737 Dump PDF VCE	650-667 Dump PDF VCE
100-105 Dump PDF VCE	352-001 Dump PDF VCE	642-742 Dump PDF VCE	650-669 Dump PDF VCE
200-001 Dump PDF VCE	400-051 Dump PDF VCE	642-883 Dump PDF VCE	650-752 Dump PDF VCE
200-105 Dump PDF VCE	400-101 Dump PDF VCE	642-885 Dump PDF VCE	650-756 Dump PDF VCE
200-120 Dump PDF VCE	400-151 Dump PDF VCE	642-887 Dump PDF VCE	650-968 Dump PDF VCE
200-125 Dump PDF VCE	400-201 Dump PDF VCE	642-889 Dump PDF VCE	700-001 Dump PDF VCE
200-150 Dump PDF VCE	400-251 Dump PDF VCE	642-980 Dump PDF VCE	700-037 Dump PDF VCE
200-155 Dump PDF VCE	400-351 Dump PDF VCE	642-996 Dump PDF VCE	700-038 Dump PDF VCE
200-310 Dump PDF VCE	500-006 Dump PDF VCE	642-997 Dump PDF VCE	700-039 Dump PDF VCE
200-355 Dump PDF VCE	500-007 Dump PDF VCE	642-998 Dump PDF VCE	700-101 Dump PDF VCE
200-401 Dump PDF VCE	500-051 Dump PDF VCE	642-999 Dump PDF VCE	700-104 Dump PDF VCE
200-601 Dump PDF VCE	500-052 Dump PDF VCE	644-066 Dump PDF VCE	700-201 Dump PDF VCE
210-060 Dump PDF VCE	500-170 Dump PDF VCE	644-068 Dump PDF VCE	700-205 Dump PDF VCE
210-065 Dump PDF VCE	500-201 Dump PDF VCE	644-906 Dump PDF VCE	700-260 Dump PDF VCE
210-250 Dump PDF VCE	500-202 Dump PDF VCE	646-048 Dump PDF VCE	700-270 Dump PDF VCE
210-255 Dump PDF VCE	500-254 Dump PDF VCE	646-365 Dump PDF VCE	700-280 Dump PDF VCE
210-260 Dump PDF VCE	500-258 Dump PDF VCE	646-580 Dump PDF VCE	700-281 Dump PDF VCE
210-451 Dump PDF VCE	500-260 Dump PDF VCE	646-671 Dump PDF VCE	700-295 Dump PDF VCE
210-455 Dump PDF VCE	500-265 Dump PDF VCE	646-985 Dump PDF VCE	700-501 Dump PDF VCE
300-070 Dump PDF VCE	500-275 Dump PDF VCE	648-232 Dump PDF VCE	700-505 Dump PDF VCE
300-075 Dump PDF VCE	500-280 Dump PDF VCE	648-238 Dump PDF VCE	700-601 Dump PDF VCE
300-080 Dump PDF VCE	500-285 Dump PDF VCE	648-244 Dump PDF VCE	700-602 Dump PDF VCE
300-085 Dump PDF VCE	500-290 Dump PDF VCE	648-247 Dump PDF VCE	700-603 Dump PDF VCE
300-101 Dump PDF VCE	500-801 Dump PDF VCE	648-375 Dump PDF VCE	700-701 Dump PDF VCE
300-115 Dump PDF VCE	600-199 Dump PDF VCE	648-385 Dump PDF VCE	700-702 Dump PDF VCE
300-135 Dump PDF VCE	600-210 Dump PDF VCE	650-032 Dump PDF VCE	700-703 Dump PDF VCE
300-160 Dump PDF VCE	600-211 Dump PDF VCE	650-042 Dump PDF VCE	700-801 Dump PDF VCE
300-165 Dump PDF VCE	600-212 Dump PDF VCE	650-059 Dump PDF VCE	700-802 Dump PDF VCE
300-180 Dump PDF VCE	600-455 Dump PDF VCE	650-082 Dump PDF VCE	700-803 Dump PDF VCE
300-206 Dump PDF VCE	600-460 Dump PDF VCE	650-127 Dump PDF VCE	810-403 Dump PDF VCE
300-207 Dump PDF VCE	600-501 Dump PDF VCE	650-128 Dump PDF VCE	820-424 Dump PDF VCE
300-208 Dump PDF VCE	600-502 Dump PDF VCE	650-148 Dump PDF VCE	840-425 Dump PDF VCE
300-209 Dump PDF VCE	600-503 Dump PDF VCE	650-159 Dump PDF VCE	
300-210 Dump PDF VCE	600-504 Dump PDF VCE	650-281 Dump PDF VCE	
300-320 Dump PDF VCE	640-692 Dump PDF VCE	650-393 Dump PDF VCE	
300-360 Dump PDF VCE	640-875 Dump PDF VCE	650-472 Dump PDF VCE	
300-365 Dump PDF VCE	640-878 Dump PDF VCE	650-474 Dump PDF VCE	
300-370 Dump PDF VCE	640-911 Dump PDF VCE	650-575 Dump PDF VCE	
300-375 Dump PDF VCE	640-916 Dump PDF VCE	650-621 Dump PDF VCE	
300-465 Dump PDF VCE	642-035 Dump PDF VCE	650-663 Dump PDF VCE	
300-470 Dump PDF VCE	642-732 Dump PDF VCE	650-665 Dump PDF VCE	
300-475 Dump PDF VCE	642-747 Dump PDF VCE	650-754 Dump PDF VCE	

HOT EXAMS

Cisco

100-105 Dumps VCE PDF
200-105 Dumps VCE PDF
300-101 Dumps VCE PDF
300-115 Dumps VCE PDF
300-135 Dumps VCE PDF
300-320 Dumps VCE PDF
400-101 Dumps VCE PDF
640-911 Dumps VCE PDF
640-916 Dumps VCE PDF

Microsoft

70-410 Dumps VCE PDF
70-411 Dumps VCE PDF
70-412 Dumps VCE PDF
70-413 Dumps VCE PDF
70-414 Dumps VCE PDF
70-417 Dumps VCE PDF
70-461 Dumps VCE PDF
70-462 Dumps VCE PDF
70-463 Dumps VCE PDF
70-464 Dumps VCE PDF
70-465 Dumps VCE PDF
70-480 Dumps VCE PDF
70-483 Dumps VCE PDF
70-486 Dumps VCE PDF
70-487 Dumps VCE PDF

CompTIA

220-901 Dumps VCE PDF
220-902 Dumps VCE PDF
N10-006 Dumps VCE PDF
SY0-401 Dumps VCE PDF