

# ***KillTest***

Higher Quality, Better Service!



## **Q&A**

<http://www.killtest.com>

We offer free update service for one year.

**Exam** : **156-815.70**

**Title** : Check Point Certified  
Managed Security Expert  
R70

**Version** : Demo

1.Which operating system listed supports running a Multi-Domain Management with Provider-1 MDS, but has a limitation in the number of virtual IP addresses which can be assigned to a given interface?

- A. Red Hat Enterprise Linux
- B. Windows 2003 Server
- C. SecurePlatform
- D. Solaris

**Answer: D**

2.Which of the following systems would meet the MINIMUM requirements for an MDS.?

- A. SecurePlatform, 10 GB hard drive
- B. SecurePlatform, 2-GB hard drive, 8 MB memory
- C. Solaris 9, 4-GB hard drive, 1 GB memory
- D. Linux RHEL 5, 2.4 kernel, 4-GB hard drive, 4-GB memory

**Answer: A**

3.Which of the following are valid reasons for using Multi-Domain Management with Provider-1 instead of Management Servers?

- 1. Customer Security
- 2. Global Properties (NOT Global Policies)
- 3. Enhanced packet inspection
- 4. Centralized management

- A. 3 and 4
- B. 2 and 3
- C. 1 and 3
- D. 1 and 4

**Answer: D**

4.A Multi-Domain Management with Provider-1 MDS is supported on which of the following platforms?

- 1. SecurePlatform
- 2. Solaris
- 3. Windows
- 4. IPSO/FreeBSD

- A. 1, 2, and 3
- B. 2 and 3
- C. 1 and 2
- D. 1, 2, and 4

**Answer: C**

5.Which of the following statements is TRUE about Multi-Domain Management with Provider-1?

- A. Provider-1 encrypts all traffic among modules - so no firewall is necessary to protect the Provider-1 system.
- B. The MDS Manager has a built-in firewall for the Provider-1 system, protecting the MDS Containers.

C. The added security of a firewall to protect the Provider-1 system is difficult to implement, and is not recommended.

D. A separately managed Security Gateway is recommended to protect the Provider-1 environment.

**Answer: D**

6. On which SecurePlatform kernel version is Multi-Domain Management with Provider-1 R70 built?

A. 2.4.18

B. 2.6.18-92

C. 2.4.21-21

D. RHEL 3

**Answer: B**

7. What is the name for the interface connecting CMA Virtual IPs?

A. Leading VIP Interface

B. VIP Lounge Interface

C. Main External Interface

**Answer: A**

8. Communication between the MDG and the MDS is secured in what way?

A. IKE encryption using shared secret

B. Configurable third-party authentication mechanism

C. Username and Password authentication

D. SSL initiated using SIC certificate exchange

**Answer: D**

9. All of the following can be configured on a Multi-Domain Management with Provider-1 MDS, EXCEPT:

A. Analyze logs

B. Firewall Module

C. Firewall Manager

D. Customer Logging Module

**Answer: B**

10. When does a SIC certificate expire for CMA/MDS?

A. After 3 years

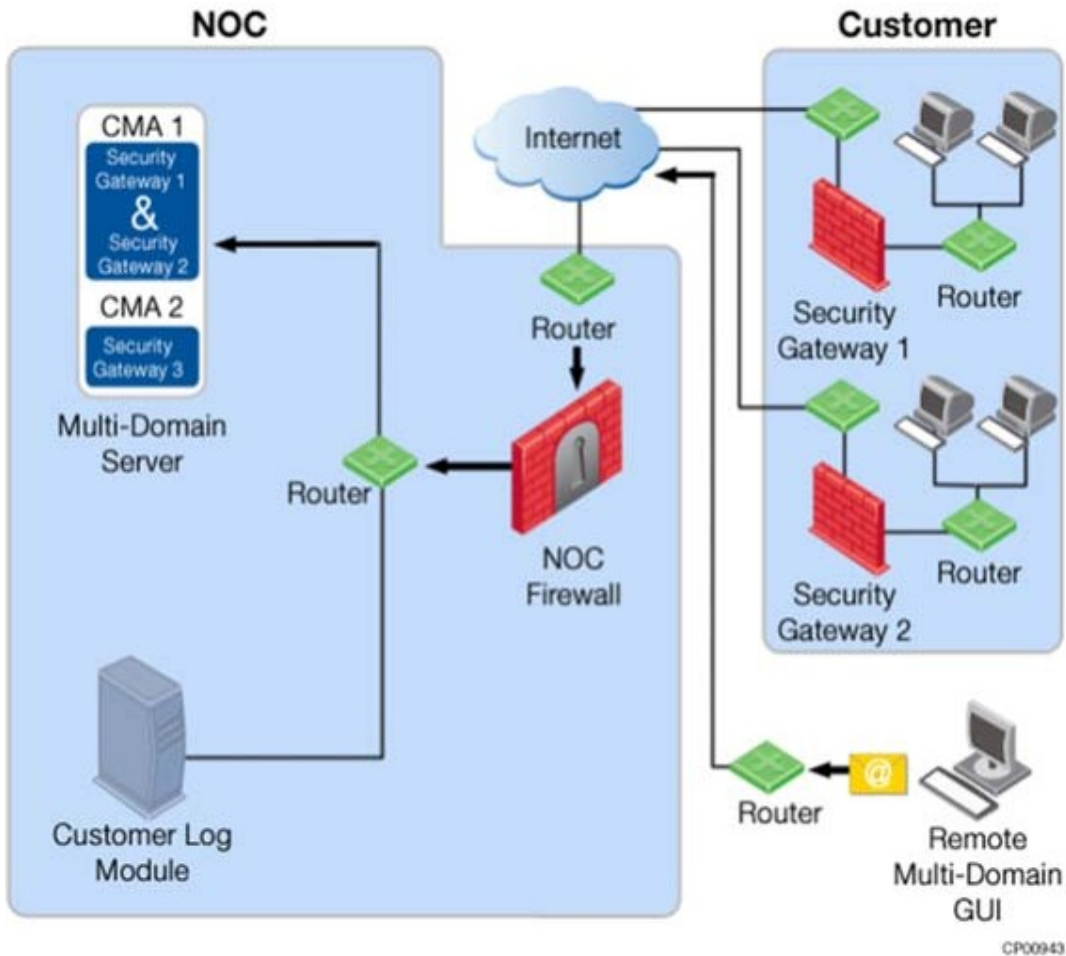
B. After 5 years

C. The interval is configurable.

D. After 1 year

**Answer: B**

11. When a NOC firewall separates the Multi-Domain Management with Provider-1 MDS machine and the MDG (as shown below), what must be done to allow the MDG to connect to the MDS?



Modify the NOC Security Gateway Rule Base to allow:

- A. RPC traffic for the MDG.
- B. CPD and CPD\_amon traffic to pass between the MDG and the MDS.
- C. UDP traffic for the MDG.
- D. CPMI traffic to pass between the MDG and the MDS.

**Answer: D**

12. Which of the following ports is used by CPMI to communicate between Multi-Domain Management with Provider-1 modules?

- A. TCP port 260
- B. TCP port 264
- C. TCP port 18191
- D. TCP port 18190

**Answer: D**

13. When debugging the fwm process at the MDS level, what file is created?

- A. \$FWDIR/log/fwm.elg and fwm.log
- B. /var/opt/CPsuite-R70/fw1/log/mds.elg and /var/opt/CPmds-R70/log/mds.log
- C. /var/opt/CPsuite-R70/fw1/log/fwm.elg and fwm.log
- D. \$CPDIR/log/debug.elg

**Answer: B**

14. When debugging the fwm process at the MDS level, what file is created?

- A. fwm.log
- B. mds.error
- C. mds.log
- D. fwm.elg

**Answer: C**

15. What information can NOT be obtained from the mdsstat output?

- A. Hostname of the MDS
- B. Up / down status
- C. IP address of the CMA
- D. PID number FWD

**Answer: A**

16. Upon boot, where is the script for the automatic start of the MDS processes located?

- A. /etc/init.d
- B. /var/init.d
- C. etc/init.D
- D. var/etc/init.d

**Answer: A**

17. Which one of the processes runs on the MDS Level?

- A. fwm mds
- B. fgd
- C. iked
- D. vpnd

**Answer: A**

18. What directory is shared between MDS and CMA?

- A. \$FWDIR/log
- B. \$FWDIR/database
- C. \$FWDIR/bin
- D. \$FWDIR/conf

**Answer: C**

19. Where do the Global Policy database files reside in an MDS environment?

- A. \$CPDIR/conf
- B. \$MDSDIR/database
- C. \$MDSDIR/conf/mdsdb
- D. \$MDSDIR/conf

**Answer: D**

20. What directory would you find all the configuration files related to the CMA "Customer\_1"?

A. /opt/CPmnds-R70/Customer\_1/

B. /opt/CPmnds-R70/customers/Customer\_1/CPsuite-R70/conf

C. /opt/CPmnds-R70/customers/Customer\_1/CPsuite-R70/fw1/conf

D. /opt/CPmnds-R70/customers/Customer\_1/CPsuite-R70/

**Answer:** A