250-501

Symantec

Intrusion Protection Solution Exam

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 250-501 exam in first attempt and also get high scores to acquire Symantec certification.

If you use OfficialCerts 250-501 Certification questions and answers, you will experience actual 250-501 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Symantec exam prep covers over 95% of the questions and answers that may be appeared in your 250-501 exam. Every point from pass4sure 250-501 PDF, 250-501 review will help you take Symantec 250-501 exam much easier and become Symantec certified.

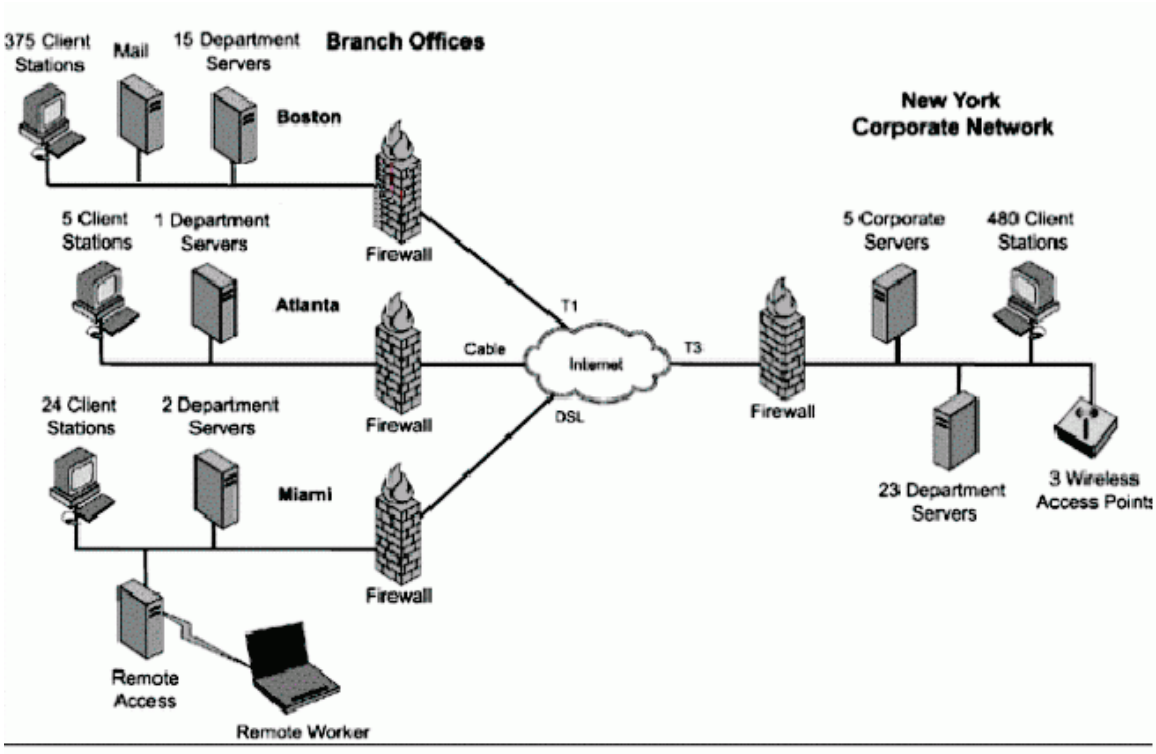
Here's what you can expect from the OfficialCerts Symantec 250-501 course:

** Up-to-Date Symantec 250-501 questions as experienced in the real exam.*
** 100% correct Symantec 250-501 answers you simply can't find in other 250-501 courses.*
** All of our tests are easy to download. Your file will be saved as a 250-501 PDF.*
** Symantec 250-501 brain dump free content featuring the real 250-501 test questions.*

Symantec 250-501 certification exam is of core importance both in your Professional life and Symantec certification path. With Symantec certification you can get a good job easily in the market and get on your path for success. Professionals who passed Symantec 250-501 exam training are an absolute favorite in the industry.
You will pass Symantec 250-501 certification test and career opportunities will be open for you.

http://news.ift.org/?newsid=exams.asp?examcode=250-501

Question: 1
Exhibit



What should you do so that one out of three attempts to gain access to a server on the Boston network ends up in a cage on a Symantec Decoy Server?

A.Deploy one Symantec Decoy Server on the Boston Network, configure the Symantec Decoy Server with four cages.
B.Deploy two Symantec Decoy Server on the Boston Network, configure four cages on one Symantec decoy Server and two cages on the other Symantec Decoy Server
C. Deploy two Symantec Server on the Boston Network, configure three cages on one Symntec Decoy. Server and two cages on the other Symantec Decoy Server.
D. Deploy ne Symantec Decoy Server on the Boston Network; configure the Symantec Decoy Server with three cages; configure the firewall to send one third of netwkork to the cages.

Answer: C

Explanation:
Note: Diagram on exam did not have mail server.

Question: 2
Symantec Decoy Server offers a unique advantage in detecting which type of intrusion?

A.A slow scan
B.A brute force attack
C.A local buffer overflow
D.A distributed denial of service

Answer: A

Explanation:
Page 8Symantec Decoy Server 3.1Student ManualNovember 7, 2003 Finally, a honeypot can detect and record incidents that might last for months. These "slow scans" are difficult to detect usingan IDSbecause the duration involved makes them appear to be normal traffic.

Question: 3
What are two advantages of hosting multiple cages on Symantec Decoy Server? (Choose two.)

A.Network traffic is reduced.
B.There is greater ease of administration.
C.Each cage shares a network interface.
D.The cost of creating a deception network is reduced.

Answer: B, D

Explanation:
Page 42Symantec Decoy Server 3.1Student ManualNovember 7, 2003 Cages are virtual environments that attackers can explore and change.Symantec Decoy Server allows a single machine to host up to four cages, which reduces the costs associated with implementing a deception network.Although the configuration options are endless, a sample configuration would have each cage mimic an organization's FTP, HTTP, SMTP, or SQL servers. This capability greatly reduces hardware costs, while increasing the probability of an attack to a cage rather than an actual server. Each cage requires a dedicated network interface and has a unique IP address [which indicates that option C is incorrect].

Question: 4
What kind of deployment is created if you have configured a router or firewall to redirect attacks against high-value targets to Symantec Decoy Server?

A.Shield deployment
B.Stealth deployment
C.Minefield deployment
D.Redirection deployment

Answer: A

Explanation:
Page 11 Symantec Decoy Server 3.1 Implementation Guide The shield deployment scheme uses a redirection device to redirect attacks against high-value targets to Symantec Decoy Server.

Question: 5
Which two benefits does Symantec Decoy Server provide? (Choose two.)

A.Zero day attack detection
B.Real-time network sniffing
C.Early warning Intrusion sensors
D.Improved host-based intrusion performance

Answer: A, C

Explanation:
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=157
Symantec Decoy Server provides early detection of internal, external, and unknown attacks, unauthorized use of passwords and server access to help prioritize threats, and increased

network protection against intrusions. Page 48Symantec Decoy Server 3.1Student ManualNovember 7, 2003 Decoy Server provides the following:

1.Early warning system
2.Unauthorized access and misuse detection
3.Zero-day attack detection
4.Network and kernel-level logging
5.Secure confinement area (attack actions logged and monitored)

Question: 6
Which two can be collected from the Symantec Decoy Server console? (Choose two.)

A.Virus activity
B.Network activity
C.Process history
D.Source quenching

Answer: B, C

Explanation:
Page 48Symantec Decoy Server 3.1Student ManualNovember 7, 2003 Decoy Server can detect and isolate malicious behavior through the following:
1.Network activity
2.File system activity
3.Process activity
4.Kernel-level keystroke capture
Page 103 Symantec Decoy Server 3.1 Implementation Guide
Cage log data
1.All Records-Displaysall cage log records.
2.PTY Session Activity-Displaysall activity that occurred during an established PTY (pseudo teletype) session with a cage. For example, if an intruder successfully telnets to a cage, all keystrokes entered and output to the screen are recorded as PTYSessionActivity.
3.File System Activity-Displaysthe names of all files opened for writing.
4.Invoked Processes-Displaysall processes that have been executed within the cage.
5.Network Activity-Displays www.PrometricVUE.comwww. Leading the way in IT testing and certification tools, www.Examsheets.in
6 all incoming UDP or TCP connections, as well as connection attempts. Incoming connections includetrlnetconnections, FTP connections, and port scans. These log records will contain the source and destination IP addresses and ports.

Question: 7
With which solution does Symantec Decoy Server integrate?

A.Symantec Host IDS
B.Symantec Man Hunt™
C.Symantec Enterprise Firewall
D.Symantec Enterprise Security Manager

Answer: B

Explanation:
Page 4Symantec Decoy Server 3.1 Implementation Guide
Symantec Decoy Server can also send events to Symantec ManHunt™, enabling you to monitor Decoy Server and ManHunt events from a single console as well as configuring ManHunt responses to decoy server events.

OfficialCerts.com Certification Exam Full Version Features;

- Verified answers researched by industry experts.
- Exams **updated** on regular basis.
- Questions, Answers are downloadable in **PDF** format.
- **No authorization** code required to open exam.
- **Portable** anywhere.
- 100% success ***Guarantee***.
- **Fast**, helpful support 24x7.

View list of All exams we offer;
http://www.officialcerts.com/allexams.asp

To contact our Support;
http://www.officialcerts.com/support.asp

View FAQs
http://www.officialcerts.com/faq.asp

Download All Exams Samples
http://www.officialcerts.com/samples.asp

To purchase Full Version and updated exam;
http://www.officialcerts.com/allexams.asp

Shop now using PayPal

3COM	CompTIA	Filemaker	IBM	LPI	OMG	Sun
ADOBE	ComputerAssociates	Fortinet	IISFA	McAfee	Oracle	Sybase
APC	CWNP	Foundry	Intel	McData	PMI	Symantec
Apple	DELL	Fujitsu	ISACA	Microsoft	Polycom	TeraData
BEA	ECCouncil	GuidanceSoftware	ISC2	Mile2	RedHat	TIA
BICSI	EMC	HDI	ISEB	NetworkAppliance	Sair	Tibco
CheckPoint	Enterasys	Hitachi	ISM	Network-General	SASInstitute	TruSecure
Cisco	ExamExpress	HP	Juniper	Nokia	SCP	Veritas
Citrix	Exin	Huawei	Legato	Nortel	See-Beyond	Vmware
CIW	ExtremeNetworks	Hyperion	Lotus	Novell	Google