

643-531

Cisco

Cisco Secure Intrusion Detection Systems

OfficialCerts.com is a reputable IT certification examination guide, study guides and audio exam provider. We ensure that you pass your 643-531 exam in first attempt and also get high scores to acquire Cisco certification.

If you use OfficialCerts 643-531 Certification questions and answers, you will experience actual 643-531 exam questions/answers. We know exactly what is needed and have all the exam preparation material required to pass the exam. Our Cisco exam prep covers over 95% of the questions and answers that may be appeared in your 643-531 exam. Every point from pass4sure 643-531 PDF, 643-531 review will help you take Cisco 643-531 exam much easier and become Cisco certified.

Here's what you can expect from the OfficialCerts Cisco 643-531 course:

- * Up-to-Date Cisco 643-531 questions as experienced in the real exam.*
- * 100% correct Cisco 643-531 answers you simply can't find in other 643-531 courses.*
- * All of our tests are easy to download. Your file will be saved as a 643-531 PDF.*
- * Cisco 643-531 brain dump free content featuring the real 643-531 test questions.*

Cisco 643-531 certification exam is of core importance both in your Professional life and Cisco certification path. With Cisco certification you can get a good job easily in the market and get on your path for success. Professionals who passed Cisco 643-531 exam training are an absolute favorite in the industry. You will pass Cisco 643-531 certification test and career opportunities will be open for you.

<http://janetdailey.com/?certs=exams.asp?examcode=643-531>



Note:

Section A contains 58 questions

Section B contains 80 questions.

The total numbers of questions is 138

Each section starts with Question NO 1.

Section A

QUESTION NO: 1

Which statement is true regarding the IDS Sensor communications?

- A. RDEP uses SSL for secured internal communications.
- B. RDEP uses SSH for secure external communications.
- C. PostOffice protocol uses IPSec for secured external communications.
- D. IDAPI uses HTTPS for secured internal communications.
- E. cidCU uses SSH for secured external communications.

Answer: A

Explanation:

Data Acquisition

The Cisco IDS **RDEP** Info Mediator acquires data from the **RDEP** server across a secure TCP link using SSL. This data is held in IDIOM XML format (Cisco's XML format). The Cisco IDS **RDEP** Info Mediator parses the data into events and sends them to the Cisco Info Server.

B RDEP does not use SSH for external communications

C PostOffice protocol does not encrypt

PostOffice Features

The **PostOffice protocol** provides a critical communication link between your Director platform and your IDS sensors. Being the primary method of communication, the **PostOffice protocol** must support certain necessary functionality:

- Reliability
- Redundancy
- Fault tolerance

D IDAPI I COULDN'T FIND ANYTHING ABOUT IDAPI AND HTTPS

E and nothing for E

Reference:

http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/products_technical_reference_chapter09186a00801c847a.html

QUESTION NO: 2

What is the purpose of the PuTTYgen utility in IDS MC?

- A. Generates SSL certificates for IDS Sensors.
- B. Generates SSH public and private keys for IDS Sensors.
- C. Generates SSH public and private keys for IDS MC server.
- D. Generates shared secret keys for IDS Sensors and IDS MC server.
- E. Generates SSL keys for administrative client access to IDS MC server.

Answer: C

Explanation:

To use SSH keys in IDS MC or Security Monitor, follow these steps:

Step 1 To use SSH keys in IDS MC or Security Monitor for Windows 2000, follow these steps:

- a. Use PuttyGen to generate your keys. Instructions are available at <http://www.chiark.greenend.org.uk/~sgtatham/putty/docs.html> .
- b. Copy the public key to the sensor's ~/.ssh/authorized_keys file.
- c. Save the private key. We recommend the name sensorname.key for the private key and we use it in this example.

Reference:

http://www.cisco.com/en/US/products/sw/cscowork/ps3990/products_user_guide_chapter09186a008018d972.html

QUESTION NO: 3

Exhibit:



Refer to the exhibit. Server TestKing 4 is in VLAN 8. The Catalyst 6500 is running Catalyst OS. Which command represents a valid configuration step to permit the ISDM2 to monitor traffic sent to and from VLAN3, VLAN4, and VLAN5?

Leading the way in IT testing and certification tools, www.testking.org

- A. 6500(config)# **monitor session 1 source vlan 3, 4, 5**
- B. 6500(config)# **monitor session 1 source 3-5 both**
- C. 6500(config)# **monitor session 1 destination idsm**
- D. 6500>(enable) **set span 3 –5 8/1 both**
- E. 6500>(enable) **set span source vlan-list 3 – 5 destination interface 8/1 both create**

Answer: A

Explanation:

Switch(config)# **monitor session** {session_number} {**source** {**interface** type/num} | {**vlan** vlan_ID}} [, | - | **rx** | **tx** | **both**]

Specifies the SPAN session number (1 through 6), the source interfaces (FastEthernet or GigabitEthernet), or VLANs (1 through 1005), and the traffic direction to be monitored.

Reference:

[Configuring SPAN](#)

QUESTION NO: 4

Match the most appropriate filtering method to the capture configuration that restricts the VLANs monitored on a trunk port. Use each option only once.

Clear trunk and set trunk commands	place here
filter keyword in set rspan command	place here
allow vlan keyword in switchport capture command	place here
filter keyword in monitor session command	place here

Use these

Catalyst OS using remote SPAN	Catalyst IOS using remote SPAN
Catalyst OS using VACLs	Catalyst IOS using mls ip ids

Answer:

Clear trunk and set trunk commands	Catalyst OS using VACLs
filter keyword in set rspan command	Catalyst OS using remote SPAN
allow vlan keyword in switchport capture command	Catalyst IOS using remote SPAN
filter keyword in monitor session command	Catalyst IOS using mls ip ids

Comment:

Clear trunk and set trunk commands -----> [Catalyst OS using VACLs]

filter keyword in set rspan command ---> [Catalyst OS using remote SPAN]

allow vlan keyword in switchport capture command -----> [Catalyst IOS using remote SPAN]

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/12_1e/swconfig/span.pdf

Section : Local SPAN and RSPAN Guidelines and Restrictions

filter keyword in monitor session command -----> [Catalyst IOS using mls ip ids]

Refer to :http://psyber.letifer.org/downloads/priv/cisco_switch_commands.pdf

QUESTION NO: 5

Which type of signature engine is characterized by single packet conditions?

- A. other
- B. string
- C. atomic
- D. traffic

Answer: C**Signature Structure**

As previously discussed, signature implementations deal with packet headers and packet payloads. The structure of the signatures deals with the number of packets that must be examined to trigger an alarm. Two types of signature structures exist and these are as follows:

- Atomic
- Composite

Atomic Structure

Some attacks can be detected by matching IP header information (context based) or string information contained in a single IP packet (content based). **Any signatures that can be matched with a single packet fall into the atomic category.** Because atomic signatures examine individual packets, there's no need to collect or store state information.

An example of an atomic signature is the SYN-FIN signature (signature ID 3041).

This signature looks for packets that have both the SYN and FIN flags set. The *SYN flag* indicates this is a packet attempting to begin a new connection. The *FIN flag* indicates this packet is attempting to close an existing connection. These two flags shouldn't be

Leading the way in IT testing and certification tools, www.testking.org

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	

You have made the
Right Choice

You are becoming member of most comprehensive, accurate, highest quality and lowest cost certification resource in the world.

