

JN0-541^{Q&As}

IDP, Associate(JNCIA-IDP)

Pass Juniper JN0-541 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/jn0-541.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Juniper
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

When Address Resolution is enabled in the Log Viewer, which machine is responsible for performing the DNS Lookups?

- A. IDP Sensor
- B. WHOIS Servers
- C. IDP User Interface
- D. IDP Management Server

Correct Answer: B

flag	alarm	time received	attack	action	source address	src port	destination address	dst port
		3/15/06 6:59:09 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3206	64.34.169.61	http
		3/15/06 6:59:18 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 6:59:23 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3221	64.34.169.61	http
		3/15/06 6:59:32 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 6:59:57 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3236	64.34.169.61	http
		3/15/06 7:00:06 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 7:00:13 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3252	64.34.169.61	http
		3/15/06 7:00:22 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 7:01:04 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3294	64.34.169.61	http
		3/15/06 7:01:14 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 7:01:18 AM	Spyware: 123Mania	drp packet	ZERO-ONE	3315	64.34.169.61	http
		3/15/06 7:01:28 AM	Spyware: 123Mania	drp packet	ZERO-ONE	0	64.34.169.61	http
		3/15/06 11:52:49 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18005	tm.wc.ask.com	http
		3/15/06 11:52:57 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	0	0.0.0.0	http
		3/15/06 11:53:21 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18031	cm.wc.ask.com	http
		3/15/06 11:53:42 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18042	cm.wc.ask.com	http
		3/15/06 11:55:48 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18094	cm.wc.ask.com	http
		3/15/06 11:55:57 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	0	0.0.0.0	http
		3/15/06 11:56:21 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18104	cm.wc.ask.com	http
		3/15/06 11:56:42 AM	Spyware: ExactSearch	drp packet	Bluecoat Proxy SG	18106	cm.wc.ask.com	http
		3/15/06 8:35:06 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	28091	213.214.183.199	http
		3/15/06 8:38:06 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	28421	213.214.183.199	http
		3/15/06 11:16:03 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	35746	213.214.183.199	http
		3/15/06 11:19:02 PM	Spyware: CrackSpider	drp packet	Bluecoat Proxy SG	35918	213.214.183.199	http

Summary | All Fields | Whois Lookup | Profile Information

Query: 192.187.224.228 Whois Server: whois.arin.net

OrgName: ICG-NetAhead, Inc.
 OrgID: JCGM
 Address: 161 Inverness Drive West
 City: Englewood
 StateProv: CO

QUESTION 2

What are two differences between Action and IP Action? (Choose two.)

- A. Action responds to matching traffic by dropping, or closing current attacking packets or connection.

- B. IP Action responds to matching traffic by dropping, or closing current attacking packets or connection.
- C. Action responds to future traffic based on a previous match by blocking or dropping future connections.
- D. IP Action responds to future traffic based on a previous match by blocking or closing future connections.

Correct Answer: AD

Action deals with immediate attacks and IP Actions deal with future attacks.

QUESTION 3

Which filters can be applied to reports?

- A. Source IP/Port, Destination IP Port, Protocol, Attack, Time
- B. Filters cannot be applied to reports.
- C. any field in the Log Viewer
- D. Source IP, Destination IP and Port, Protocol, Attack, Time

Correct Answer: C

QUESTION 4

What is "a signature or protocol anomaly combined with context information"?

- A. attack object
- B. context
- C. attack signature
- D. protocol anomaly

Correct Answer: A

QUESTION 5

What does a Drop Packet action do?

- A. drops any packet matching thissrc/dst/protocol
- B. drops all packets from the attacker's IP
- C. drops only the specific packet matching the attack
- D. drops the specific session containing the attack pattern

Correct Answer: C

[JN0-541 VCE Dumps](#)

[JN0-541 Exam Questions](#)

[JN0-541 Braindumps](#)