



300-207^{Q&As}

Implementing Cisco Threat Control Solutions

Pass Cisco 300-207 Exam with 100% Guarantee

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

<https://www.pass4lead.com/300-207.html>

100% Passing Guarantee
100% Money Back Assurance

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

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





QUESTION 1

Which Cisco Security IntelliShield Alert Manager Service component mitigates new botnet, phishing, and web-based threats?

- A. the IntelliShield Threat Outbreak Alert
- B. IntelliShield Alert Manager vulnerability alerts
- C. the IntelliShield Alert Manager historical database
- D. the IntelliShield Alert Manager web portal
- E. the IntelliShield Alert Manager back-end intelligence engine

Correct Answer: A

QUESTION 2

What three alert notification options are available in Cisco IntelliShield Alert Manager? (Choose three.)

- A. Alert Summary as Text
- B. Complete Alert as an HTML Attachment
- C. Complete Alert as HTML
- D. Complete Alert as RSS
- E. Alert Summary as Plain Text
- F. Alert Summary as MMS

Correct Answer: ABC

QUESTION 3

Which three zones are used for anomaly detection in a Cisco IPS? (Choose three.)

- A. internal zone
- B. external zone
- C. illegal zone
- D. inside zone
- E. outside zone
- F. DMZ zone



Correct Answer: ABC

QUESTION 4

Instructions

Click the grey buttons at the bottom of this frame to view the different windows.

Windows can be minimized and repositioned. You can also reposition a window by dragging it by the title bar.

Scenario

You are a network security admin with the need to apply an aggressive policy to deny high and medium risk events against traffic to and from a high value network segment, placing the IPS inline using two interfaces GigabitEthernet0/0 & GigabitEthernet0/1. You also have a requirement to further analyze lower risk events across that same network segment by capturing traffic for later inspection.

Topology

The diagram shows a network topology. On the left, there is a 'High Value Segment' represented by two red circles connected to a vertical line. A horizontal line labeled 'GigabitEthernet 0/0' connects this segment to a blue box labeled 'IPS'. From the right side of the 'IPS' box, another horizontal line labeled 'GigabitEthernet 0/1' connects to a cloud labeled 'Internet'.

ASDM

File View Help

Home Configuration Monitoring Back Forward Refresh Help

Interfaces

Configuration > Interfaces > Summary

The following is the configuration summary of the sensing interfaces. You can configure any single physical interface for promiscuous, inline interface pair combination of these modes is allowed.

Name	Details	Assigned Virtual Sensor
GigabitEthernet0/0	TX (copper)	--None--
GigabitEthernet0/1	TX (copper)	--None--
GigabitEthernet0/2	TX (copper)	--None--
GigabitEthernet0/3	TX (copper)	--None--
GigabitEthernet0/4	TX (copper)	--None--
GigabitEthernet0/5	TX (copper)	--None--
GigabitEthernet0/6	TX (copper)	--None--
GigabitEthernet0/7	TX (copper)	--None--
Management0/0	TX (copper)	--None--

Correct Answer: Steps are in below

First, enable the Gig 0/0 and Gig 0/1 interfaces:



A sensing interface must be enabled and assigned to a virtual sensor before the sensor will monitor that interface. You can enable/disable the available sensing interfaces by selecting the row(s) and clicking Enable or Disable.

Interface Name	Enabled	Mgmt Int	Media Type	Duplex	Speed	Default VLAN	Alternate TCP	Description
GigabitEthernet0/0	Yes	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/1	Yes	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/2	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/3	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/4	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/5	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/6	No	No	Tx(copper)	Auto	Auto	0	--None--	
GigabitEthernet0/7	No	No	Tx(copper)	Auto	Auto	0	--None--	
Management0/0	--N/A--	Yes	Tx(copper)	Auto	Auto	0	--None--	

Second, create the pair under the "interface pairs" tab.

You can create logical interface pair(s) for the available sensing interfaces.

Interface Pair Name: Gig0/0-Gig0/1

Select two interfaces:

- GigabitEthernet0/0
- GigabitEthernet0/1
- GigabitEthernet0/2
- GigabitEthernet0/3
- GigabitEthernet0/4

Description:

Then, apply the HIGHRISK action rule to the newly created interface pair:

Virtual Sensor Name: vs0
Description: default virtual sensor

Interfaces

Assigned	Name	Details
<input type="checkbox"/>	GigabitEthernet0/6	TX (copper)
<input type="checkbox"/>	GigabitEthernet0/7	TX (copper)
<input checked="" type="checkbox"/>	Gig 0/0 - Gig 0/1	Inline Interface Pair

Signature Definition
Signature Definition Policy: sig0

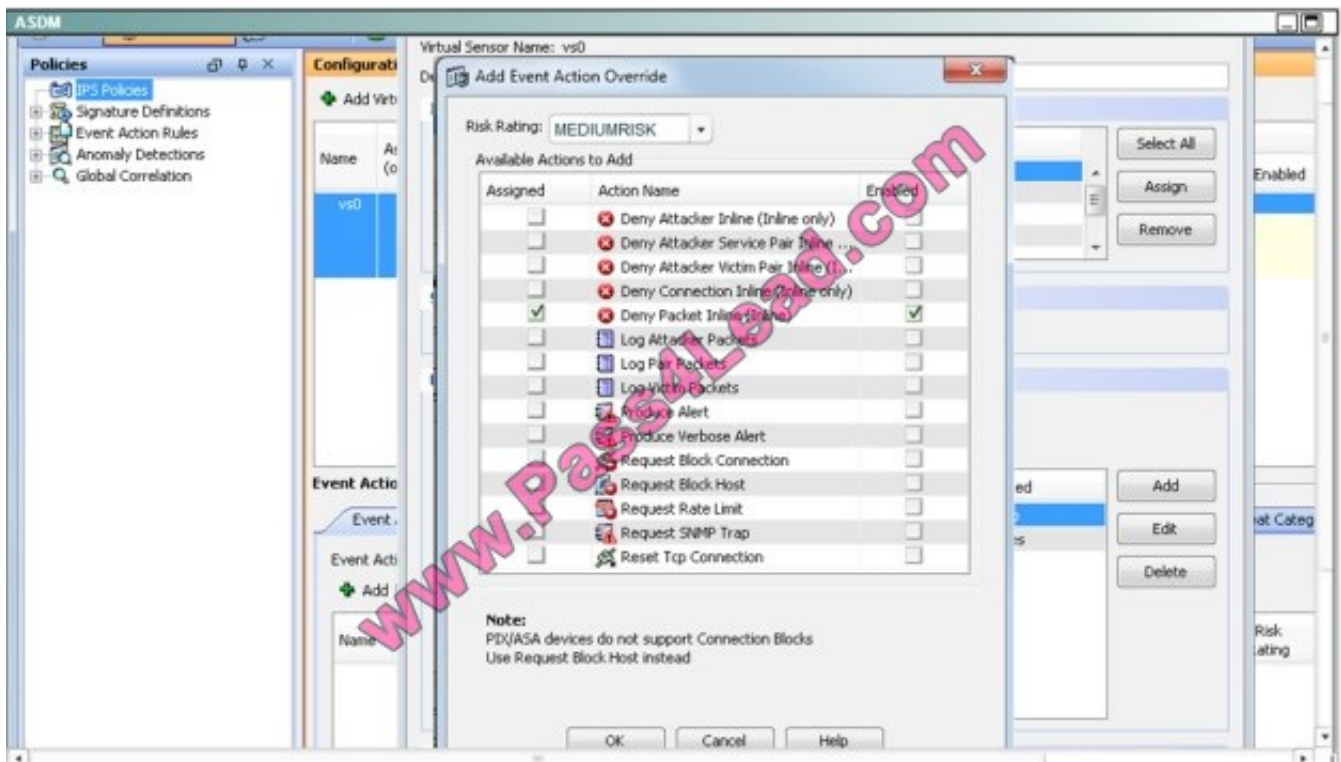
Event Action Rule
Event Action Rules Policy: rules0

Use Event Action Overrides

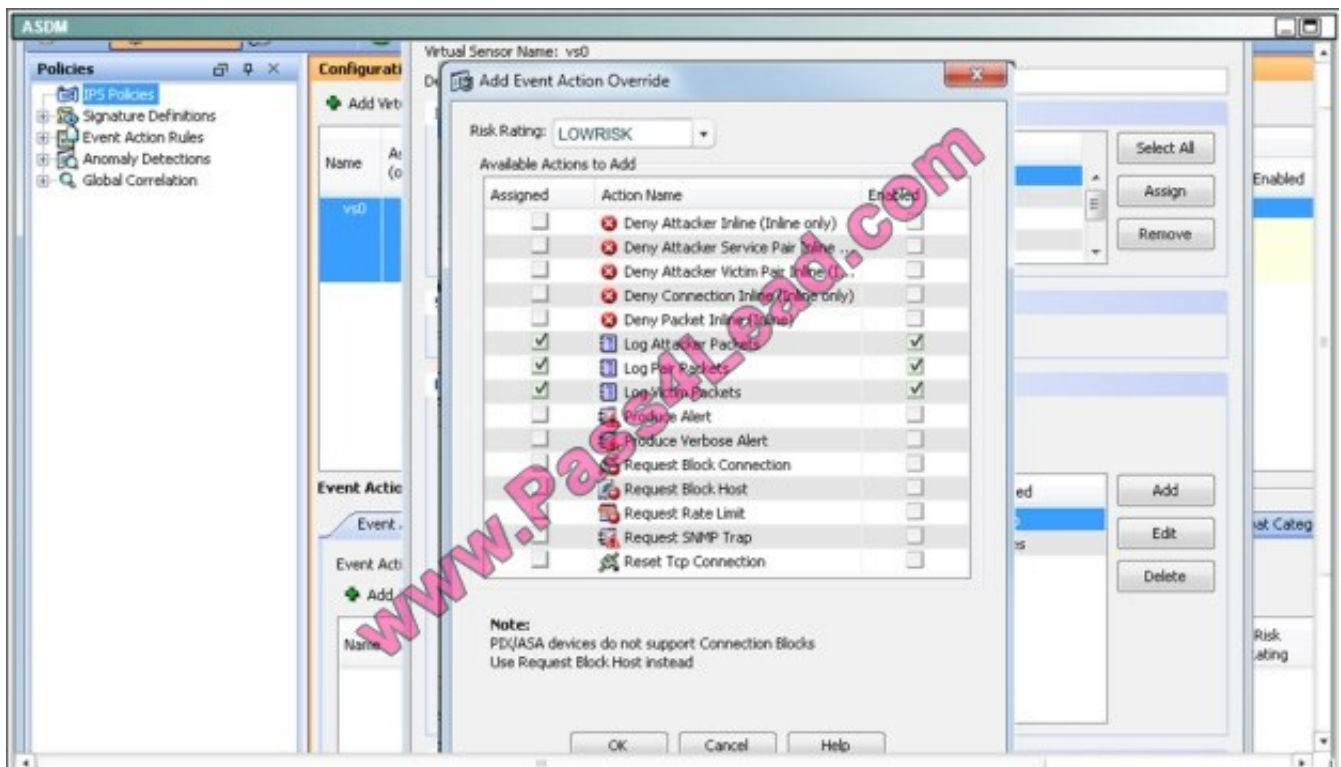
Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (inline)	Yes



Then apply the same for the MEDIUMRISK traffic (deny attacker inline)



Finally. Log the packets for the LOWRICK event:





Virtual Sensor Name: vs0
Description: default virtual sensor

Assigned	Name	Details
<input type="checkbox"/>	GigabitEthernet0/2	TX (copper)
<input type="checkbox"/>	GigabitEthernet0/3	TX (copper)
<input type="checkbox"/>	GigabitEthernet0/4	TX (copper)
<input type="checkbox"/>	GigabitEthernet0/5	TX (copper)

Signature Definition Policy: sig0

Event Action Rules Policy: rules0

Risk Rating	Actions to Add	Enabled
HIGHRISK	Deny Packet Inline (Inline)	Yes
MEDIUMRISK	Deny Packet Inline (Inline)	Yes
LOWRISK	Log Attacker Packets	Yes
	Log Pair Packets	Yes
	Log Victim Packets	Yes

Name	Assigned Interfaces (or Pairs)	Signature Definition Policy	Event Action Override Policy	Enabled	Anomaly Detection Policy	Description
vs0		sig0	rules0 (2 action overrides)		add	default virtual se...
			HIGHRISK Deny Packet Inline (Inline)	Yes		
			MEDIUMRISK Deny Packet Inline (Inline)	Yes		
			LOWRISK Log Attacker Packets	Yes		

Event Action Filters lets you **subtract** the actions associated with an event if the conditions for that event meet the criteria of the filter.

Name	Enabled	Sig ID	SubSig ID	Attacker (IPv4 / IPv6 / port)	Victim (IPv4 / IPv6 / port)	Risk Rating	Actions to Subtract

QUESTION 5

Which port is used for CLI Secure shell access?

- A. Port 23



B. Port 25

C. Port 22

D. Port 443

Correct Answer: C

[Latest 300-207 Dumps](#)

[300-207 VCE Dumps](#)

[300-207 Braindumps](#)



To Read the [Whole Q&As](#), please purchase the [Complete Version](#) from [Our website](#).

Try our product !

100% Guaranteed Success

100% Money Back Guarantee

365 Days Free Update

Instant Download After Purchase

24x7 Customer Support

Average 99.9% Success Rate

More than 800,000 Satisfied Customers Worldwide

Multi-Platform capabilities - [Windows](#), [Mac](#), [Android](#), [iPhone](#), [iPod](#), [iPad](#), [Kindle](#)

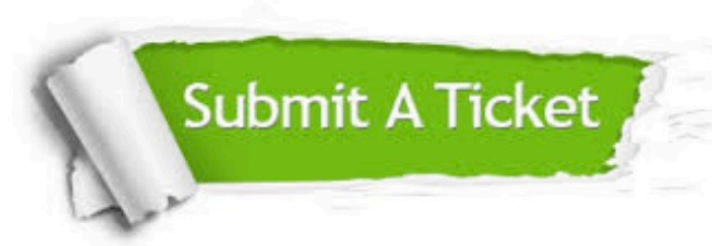
We provide exam PDF and VCE of Cisco, Microsoft, IBM, CompTIA, Oracle and other IT Certifications. You can view Vendor list of All Certification Exams offered:

<https://www.pass4lead.com/allproducts>

Need Help

Please provide as much detail as possible so we can best assist you.

To update a previously submitted ticket:



 <p>One Year Free Update Free update is available within One Year after your purchase. After One Year, you will get 50% discounts for updating. And we are proud to boast a 24/7 efficient Customer Support system via Email.</p>	 <p>Money Back Guarantee To ensure that you are spending on quality products, we provide 100% money back guarantee for 30 days from the date of purchase.</p>	 <p>Security & Privacy We respect customer privacy. We use McAfee's security service to provide you with utmost security for your personal information & peace of mind.</p>
---	---	--

Any charges made through this site will appear as Global Simulators Limited.

All trademarks are the property of their respective owners.

Copyright © pass4lead, All Rights Reserved.