642-627 Q&As

Implementing Cisco Intrusion Prevention System v7.0

Pass Cisco 642-627 Exam with 100% Guarantee

QUESTION 1

When using the Cisco IPS signature and engine auto updates feature from Cisco.com, which password must be configured on the IDM Auto/Cisco.com Update pane?

A. the IPS appliance "cisco" user account password

B. the IPS appliance "service" user account password

C. the IPS appliance "support" user account password

D. the IPS appliance enable password

E. the CCO user account password

Correct Answer: E

http://www.cisco.com/en/US/docs/security/security_management/cs-mars/6.0/device/configuration/guide/chIpsCisoc6x.html

IPS Signature Dynamic Update Settings In releases 6.0 and later, Cisco IPS supports dynamic signature updates. MARS can discover the new signatures and correctly process and categorize received events that match those signatures. If this feature is not configured, the events appears as unknown event type in queries and reports, and MARS does not include these events in inspection rules. These updates provides event normalization and event group mapping, and they enable your MARS Appliance to parse Day Zero signatures from the IPS devices. The downloaded update information is am XML file that contains the IPS signatures. However, this file does not contain detailed information, such as vulnerability information. Detailed signature information is provided in later MARS signature upgrade packages just as with 3 rd -party signatures.

Before You Begin?ynamic IPS signature updates are disabled by default. ?ustom IPS signatures are not supported. You must manually import these signatures using the process defined in Applying Custom Signature Updates.?ou can retrieve updates from CCO or from a local web server. After downloading and installing an update, the MARS Appliance performs an auto-activate to load the new signature information. ?f configured to retrieve the signatures from CCO, MARS downloads the most recent package as determined by a combination of package name and the MD5 sum. ?ARS checks for updates at the specified interval, hourly (1, 2, 3, 6, or 12) or daily (1 through 14).?n a Global Controller-Local Controller deployment, configure the dynamic signature URL and all relevant settings on the Global Controller. Do not attempt to configure these features on the Local Controllers even though the web interface allows you to do so. ?hen the Global Controller pulls the new signatures from CCO, all managed Local Controllers download the new signatures from the Global Controller.

QUESTION 2

A Cisco Catalyst switch is experiencing packet drops on a SPAN destination port that is connected to an Cisco IPS appliance. Which three configurations should be considered to resolve the packet drops issue? (Choose three.)

A. Configure an additional SPAN session to a different Cisco IPS appliance interface connected to the same virtual sensor

B. Configure an EtherChannel bundle as the SPAN destination port.

C. Configure RSPAN.

D. Configure VACL capture.

E. Configure the Cisco IPS appliance to inline mode.

Correct Answer: ADE

From Neil: A, D, E

A. Adding an additional span session to a different Cisco IPS will remove some of the traffic and load from the existing span - Confirmed Correct

B. Cisco documentation clearly defines that Ether-channels cannot be configured as SPAN destination ports.

This rules out option B. - Confirmed Incorrect

http://www.cisco.com/en/US/docs/switches/lan/catalyst3550/software/release/12.1_19_ea1/configuration/guide/swspan.html#wp1044603

C. RSPAN is remote span which is used to send traffic to a device not connected to the local switch.

While this would have a similar effect to answer A since you are in fact creating another span, the implication here is that there is only one IPS device. - Unconfirmed Incorrect D. Configuring VACL capture will allow a reduced amount of traffic

and load on the span by selecting and sending only select traffic over the SPAN to the IPS. - Confirmed Correct E. Configuring the Cisco IPS appliance in inline mode would eliminate the need for a span altogether. -Unconfirmed Correct.

Cisco ASA IPS Modules--Inline Operation

You can configure the ASA to only forward specific traffic to the AIP SSM or AIP SSC for inspection. This is achieved by using the Cisco Modular Policy Framework (MPF), where you can configure a Cisco ASA to selectively send traffic to the

AIP module operating in inline or promiscuous mode. You can also specify that all traffic be inspected by the AIP module, and if the total traffic exceeds the IPS module inspection capacity, you can modify the MPF configuration in such a way

that only critical traffic is inspected.

This approach reduces the traffic the IPS module will have to analyze, and it is guaranteed to perform optimally.

Cisco ASA IPS Modules--Promiscuous Operation

A selective capture can also be used to ensure that only part of the traffic flowing through a Cisco ASA is sent to the AIP module in promiscuous mode. This way, the AIP module is not overwhelmed and critical data is analyzed.

The same concept applies when using the Cisco IPS Advanced Integration Module (AIM):

When inline or in promiscuous mode, select traffic can be directed to it.

Cisco Catalyst Switches--VACL Capture

When an IPS is connected to a Cisco Catalyst switch, you can perform selective capture by setting the appropriate VLAN access control lists (VACL). The VACLs capture only a subset of traffic off the switch backplane and copy it to the

sensor that is connected on a capture port, instead of a SPAN port. The sensor in this case only receives a copy of the packets that are suitable for analysis and completely ignores the rest of the traffic.

Performance issues and bottlenecks should be avoided by sizing the IPS sensors adequately and ensuring that the network topology design is a good fit.

QUESTION 3

Which four networking tools does Cisco IME include that can be invoked for specific events, to learn more about attackers and victims using basic network reconnaissance? (Choose four.)

A. ping

B. traceroute

C. packet tracer

D. nslookup

E. whois

F. nmap

Correct Answer: ABDE

http://www.cisco.com/en/US/docs/security/ips/6.1/configuration/guide/ime/ime_getting_started.htm l IME also supports tools such, as ping, trace route, DNS lookup, and whois lookup for selected events

QUESTION 4

Which Cisco IPS appliance CLI command is used to display information in the IPS Event Store?

A. show config

B. show events

C. show database

D. show sdee

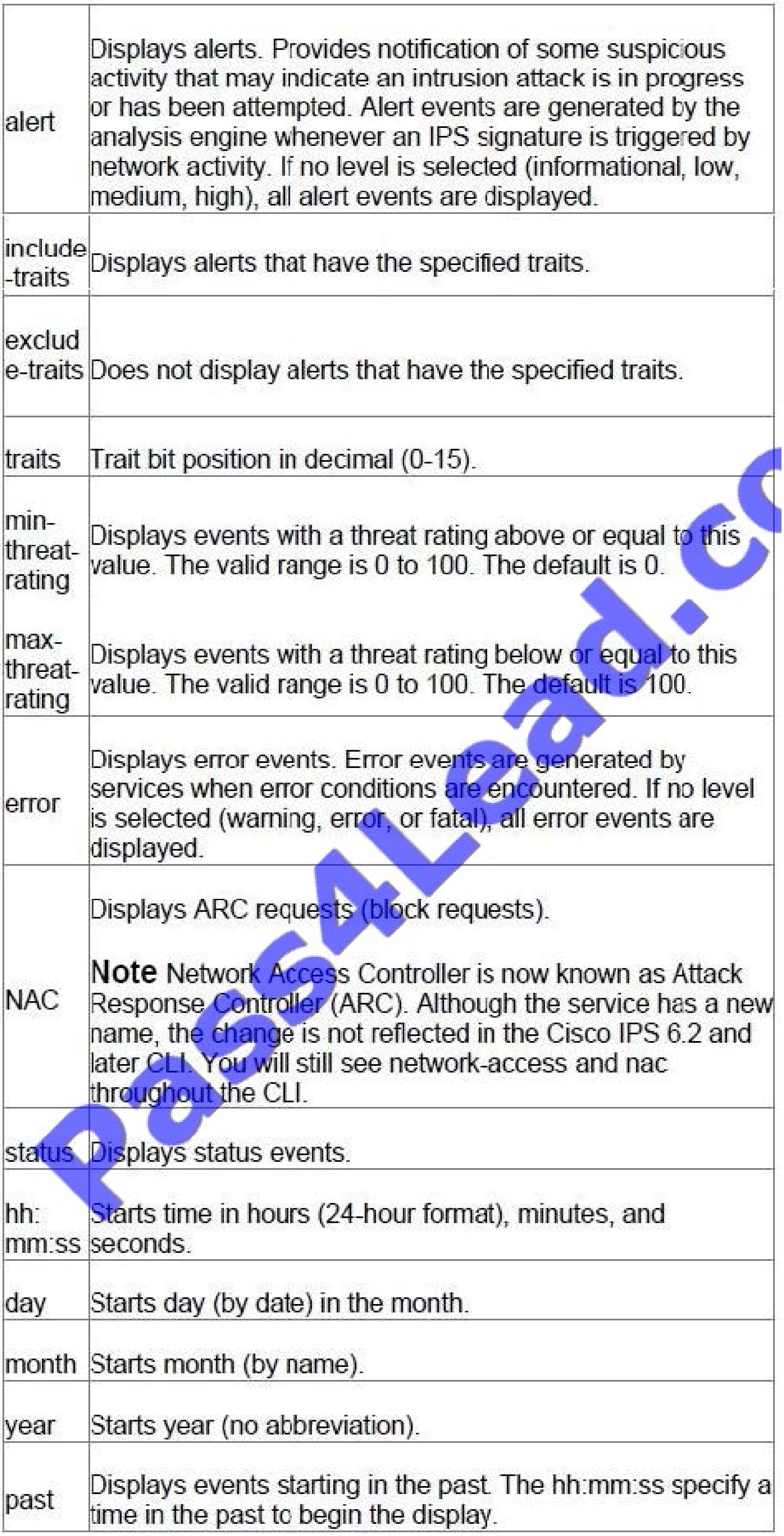
E. show log

F. show event-store

G. show alerts

Correct Answer: B

show events To display the local event log contents, use the show events command in EXEC mode. show events [{alert [informational] [low] [medium] [high] [include-traits traits] [exclude-traits traits] [min-threatrating min-rr] [max-threat-rating max-rr | error [warning] [error] [fatal] | NAC | status}] [hh:mm:ss [month day [year]] | past hh:mm:ss] Syntax Description



alert	Displays alerts. Provides notification of some suspicious activity that may indicate an intrusion attack is in progress or has been attempted. Alert events are generated by the analysis engine whenever an IPS signature is triggered by network activity. If no level is selected (informational, low, medium, high), all alert events are displayed.
include-traits	Displays alerts that have the specified traits.
exclude-traits	Does not display alerts that have the specified traits.
traits	Trait bit position in decimal (0-15).
min-threat-rating	Displays events with a threat rating above or equal to this value. The valid range is 0 to 100. The default is 0.
max-threat-rating	Displays events with a threat rating below or equal to this value. The valid range is 0 to 100. The default is 100.
error	Displays error events. Error events are generated by services when error conditions are encountered. If no level is selected (warning, error, or fatal), all error events are displayed.
NAC	Displays ARC requests (block requests). **Note** Network Access Controller is now known as Attack Response Controller (ARC). Although the service has a new name, the change is not reflected in the Cisco IPS 6.2 and later CLI. You will still see network-access and nac throughout the CLI.
status	Displays status events.
hh:mm:ss	Starts time in hours (24-hour format), minutes, and seconds.
day	Starts day (by date) in the month.
month	Starts month (by name).
year	Starts year (no abbreviation).
past	Displays events starting in the past. The hh:mm:ss specify a time in the past to begin the display.

QUESTION 5

The threat rating is calculated using which two factors? (Choose two.)

A. event action overrides

B. attack severity rating

C. risk rating

D. preventative actions taken by the Cisco IPS sensor

E. target value rating

F. attack relevancy rating

Correct Answer: CD

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5729/ps5713/ps4077/prod_white_paper0900aecd806e7299.html

To Read the Whole Q&As, please purchase the Complete Version from Our website.

Try our product !

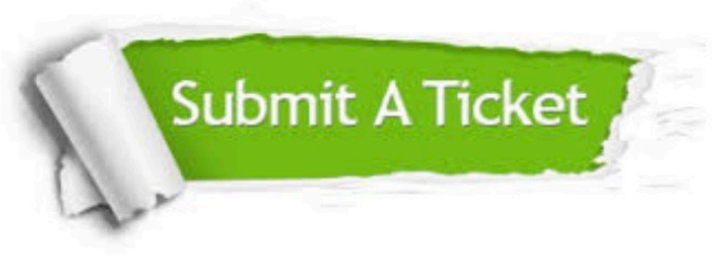
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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:



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.

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.

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.