642-618 Q&As

Deploying Cisco ASA Firewall Solutions (FIREWALL v2.0)

Pass Cisco 642-618 Exam with 100% Guarantee

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

https://www.pass4lead.com/642-618.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Refer to the exhibit.

Which reason explains why the Cisco ASA appliance cannot establish an authenticated NTP session to the inside 192.168.1.1 NTP server?

A. The ntp server 192.168.1.1 command is incomplete.

B. The ntp source inside command is missing.

C. The ntp access-group peer command and the ACL to permit 192.168.1.1 are missing.

D. The trusted-key number should be 1 not 2.

Correct Answer: A

http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/basic.html#wp106776 hostname(config)# ntp server ip_address [key key_id] [source interface_name][prefer] ntp server 192.168.1.1 2

QUESTION 2

Which two statements about traffic shaping capability on the Cisco ASA appliance are true? (Choose two.)

A. Traffic shaping can be applied to all outgoing traffic on a physical interface or, in the case of the Cisco ASA 5505 appliance, on a VLAN.

B. Traffic shaping can be applied in the input or output direction.

C. Traffic shaping can cause jitter and delay.

D. You can configure traffic shaping and priority queuing on the same interface.

E. With traffic shaping, when traffic exceeds the maximum rate, the security appliance drops the excess traffic.

Correct Answer: AC

http://www.cisco.com/en/US/docs/security/asa/asa72/configuration/guide/qos.html#wp1083655

Information About Traffic Shaping Traffic shaping is used to match device and link speeds, thereby controlling packet loss, variable delay, and link saturation, which can cause jitter and delay.

-Traffic shaping must be applied to all outgoing traffic on a physical interface or in the case of the ASA 5505, on a VLAN. You cannot configure traffic shaping for specific types of traffic. -Traffic shaping is implemented when packets are ready to be transmitted on an interface, so the rate calculation is performed based on the actual size of a packet to

be transmitted, including all the possible overhead such as the IPsec header and L2 header. -The shaped traffic includes both through-the-box and from-the-box traffic. -The shape rate calculation is based on the standard token bucket algorithm. The token bucket size is twice the Burst Size value. See the "What is a Token Bucket?" section. -When burst traffic exceeds the specified shape rate, packets are queued and transmitted later. Following are some characteristics regarding the shape queue (for information about hierarchical priority queuing, see the "Information About Priority Queuing" section):

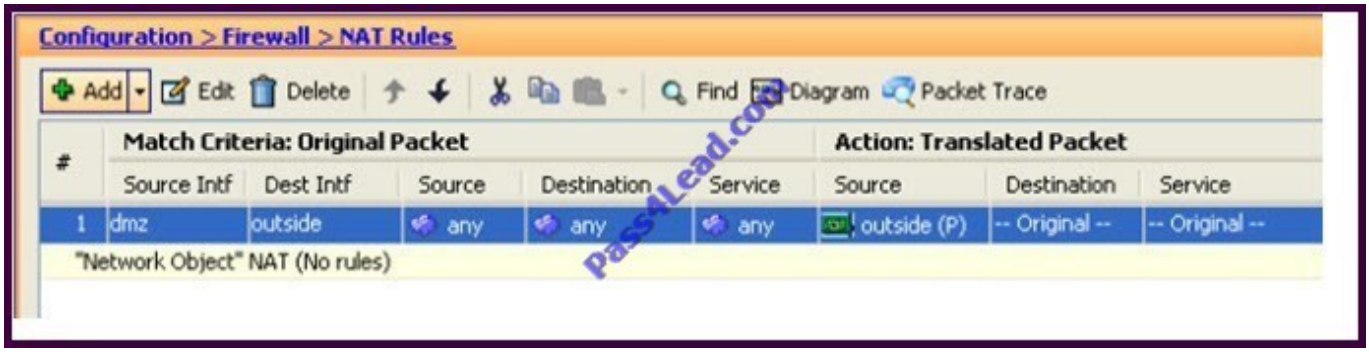
The queue size is calculated based on the shape rate. The queue can hold the equivalent of 200- milliseconds worth of shape rate traffic, assuming a 1500-byte packet. The minimum queue size is 64.

When the queue limit is reached, packets are tail-dropped. Certain critical keep-alive packets such as OSPF Hello packets are never dropped. The time interval is derived by time_interval = burst_size / average_rate. The larger the time interval is, the bustier the shaped traffic might be, and the longer the link might be idle. The effect can be best understood using the following exaggerated example:

Average Rate = 1000000 Burst Size = 1000000 In the above example, the time interval is 1 second, which means, 1 Mbps of traffic can be bursted out within the first 10 milliseconds of the 1-second interval on a 100 Mbps FE link and leave the remaining 990 milliseconds idle without being able to send any packets until the next time interval. So if there is delay sensitive traffic such as voice traffic, the Burst Size should be reduced compared to the average rate so the time interval is reduced.

QUESTION 3

Refer to the exhibit.



Which Cisco ASA CLI nat command is generated based on this Cisco ASDM NAT configuration?

A. nat (dmz, outside) 1 source static any any

B. nat (dmz, outside) 1 source static any outside

C. nat (dmz,outside) 1 source dynamic any interface

D. nat (dmz, outside) 1 source dynamic any interface destination dynamic outside outside

E. nat (dmz, outside) 1 source static any interface destination static any any

F. nat (dmz, outside) 1 source dynamic any outside destination static any any

Correct Answer: C

Pretty straight forward - like this example http://tunnelsup.com/2011/06/24/nat-for-cisco-asas-version-8-3/ Regular Dynamic PAT To create a many-to-one NAT where the entire inside network is getting PAT\\'d to a single outside IP do

the following.

Old 8.2 command: nat (inside) 1 10.0.0.0 255.255.255.0 global (outside) 1 interface New 8.3 equivalent command: object network inside-net subnet 10.0.0.0 255.255.255.0 nat (inside, outside) dynamic interface

Note: the "interface" command is the 2nd interface in the nat statement, in this case the outside.

QUESTION 4

Which statement about the Cisco ASA botnet traffic filter is true?

A. The four threat levels are low, moderate, high, and very high.

B. By default, the dynamic-filter drop blacklist interface outside command drops traffic with a threat level of high or very high.

C. Static blacklist entries always have a very high threat level.

D. A static or dynamic blacklist entry always takes precedence over the static whitelist entry.

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_botnet.html

Information About the Static Database You can manually enter domain names or IP addresses (host or subnet) that you want to tag as bad names in a blacklist. Static blacklist entries are always designated with a Very High threat level. You can also enter names or IP addresses in a whitelist, so that names or addresses that appear on both the dynamic blacklist and the whitelist are identified only as whitelist addresses in syslog messages and reports. Note that you see syslog messages for whitelisted addresses even if the address is not also in the dynamic blacklist.

QUESTION 5

Which five options are valid logging destinations for the Cisco ASA? (Choose five.)

A. AAA server

B. Cisco ASDM

C. buffer

D. SNMP traps

E. LDAP server

F. email

G. TCP-based secure syslog server

Correct Answer:

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: