

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.geekcert.com/642-618.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 ASA platform should be selected if the requirements are to support 35,000 connections per second, 600,000 maximum connections, and traffic shaping?

- A. 5540
- B. 5550
- C. 5580-20
- D. 5580-40

Correct Answer: B

http://www.cisco.com/en/US/prod/collateral/vpndevc/ps6032/ps6094/ps6120/product_data_sheet 0900aecd802930c5.pdf

Feature	Cisco ASA 5540	Cisco ASA 5550	Cisco ASA 5580-20	Cisco ASA 5580-40
Maximum Firewall and IPS	Up to 500 Mbps	Not available		CTRACTA
Throughput	with AIP-SSM-20 • Up to 650 Mbps with AIP-SSM-40	*	Unlimited	Unlimited
			10 Gbps (Max); 5 Gbps (Real- world HTTP)	20 Gbps (Max): 10 Gbps (Real- world HTTP)
3DES/AES VPN Throughput	Up to 325 Mbps	Up to 425 Mbps	1 Gbps	1 Gbps
IPsec VPN Peers	5000	5000	10,000	10,000
Premium AnyConnect VPN Peers (Included/Maximum)	2/2500	2/5000	2/10,000	2/10,000
Concurrent Connections	400,000	650,000	2,000,000	4,000,000
New Connections/Second	25,000	33,000	90,000	150,000
Integrated Network Ports	4 Gigabit Ethernet, 1 Fast Ethernet	8 Gigabit Ethernet, 4 SFP Fiber, 1 Fast Ethernet	2,500,000	4,000,000
			2-port 10/100/1000	2-port

QUESTION 2

On which type of encrypted traffic can a Cisco ASA appliance running software version 8.4.1 perform application



inspection and control?

- A. IPsec
- B. SSL
- C. IPsec or SSL
- D. Cisco Unified Communications
- E. Secure FTP

Correct Answer: D

http://www.cisco.com/en/US/solutions/collateral/ns340/ns394/ns165/ns391/guide_c07-494658.html

QUESTION 3

Which two options show the required Cisco ASA command(s) to allow this scenario? (Choose two.)

An inside client on the 10.0.0.0/8 network connects to an outside server on the 172.16.0.0/16 network using TCP and the server port of 2001. The inside client negotiates a client port in the range between UDP ports 5000 to 5500. The outside server then can start sending UDP data to the inside client on the negotiated port within the specified UDP port range.

A. access-list INSIDE line 1 permit tcp 10.0.0.0 255.0.0.0 172.16.0.0 255.255.0.0 eq 2001 access-group INSIDE in interface inside

B. access-list INSIDE line 1 permit tcp 10.0.0.0 255.0.0.0 172.16.0.0 255.255.0.0 eq 2001 access-list INSIDE line 2 permit udp 10.0.0.0 255.0.0.0 172.16.0.0 255.255.0.0 eq established access-group INSIDE in interface inside

C. access-list OUTSIDE line 1 permit tcp 172.16.0.0 255.255.0.0 eq 2001 10.0.0.0 255.0.0.0 access-list OUTSIDE line 2 permit udp 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0 eq 5000-5500 access-group OUTSIDE in interface outside

D. access-list OUTSIDE line 1 permit tcp 172.16.0.0 255.255.0.0 eq 2001 10.0.0.0 255.0.0.0 access-list OUTSIDE line 2 permit udp 172.16.0.0 255.255.0.0 10.0.0.0 255.0.0.0 eq established access-group OUTSIDE in interface outside

- E. established tcp 2001 permit udp 5000-5500
- F. established tcp 2001 permit from udp 5000-5500
- G. established tcp 2001 permit to udp 5000-5500
- Correct Answer: AG

http://www.cisco.com/en/US/docs/security/asa/asa72/command/reference/ef_72.html#wp176466 Established command--This command allows return connections from a lower security host to a higher security host if there is already an established connection from the higher level host to the lower level host.

For same security interfaces, you can configure established commands for both directions.

QUESTION 4



A Cisco ASA is operating in transparent firewall mode, but the MAC address table of the Cisco ASA is always empty, which causes connectivity issues.

What should you verify to troubleshoot this issue?

- A. if ARP inspection has been disabled
- B. if MAC learning has been disabled
- C. if NAT has been disabled
- D. if ARP traffic is explicitly allowed using EtherType ACL
- E. if BPDU traffic is explicitly allowed using EtherType ACL

Correct Answer: B

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/fwmode.html#wp1224

QUESTION 5

Refer to the exhibit.

ASA-5510# show conn
54764 in use, 54764 most used
TCP outside 172.16.1.118:26093 inside 10.1.1.50:80, idle 0:00:23, bytes 0, flags aB
TCP outside 172.16.5.19:23598 inside 10.1.1.50:80, idle 0:00:13, pytes 0, flags aB
TCP outside 192.168.1.202:32729 inside 10.1.1.50:80, idle 0:00:25, bytes 0, flags aB
TCP outside 192.168.2.20:56481 inside 10.1.1.50:80, idle 0:00:29, bytes 0, flags aB
TCP outside 192.168.3.205:18073 inside 10.1.1.50:80, idle 0.00:02, bytes 0, flags aB
TCP outside 172.16.2.63:51503 inside 10.1.1.50:80, idle 0:00:03, pytes 0, flags aB
TCP outside 172.16.18.60:47733 inside 10.1.1.50:80, tdle 0:00:27, bytes 0, flags aB
TCP outside 192.168.1.202:20773 inside 10.1.1.50:80, idle 0:00:02, bytes 0, flags aB
TCP outside 192.168.4.192:23112 inside 10.1.1.50:80, idle 0:00:06, bytes 0, flags aB
TCP outside 172.16.25.60:47733 inside 10.1.1.50:80, idle 0:00:27, bytes 0, flags aB
<pre>!<output omitted=""></output></pre>
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
B - initial SYN from outside, b - TCP state-bypass or nailed, C - CTIQBE media,
D - DNS, d - dump, E - outside back connection, F, outside FIN, f - inside FIN,
G - group, g - MGCP, H - H.323, h - H.225.0, I - inbound data,
i - incomplete, J - GTP, j - GTP data, K - GTP 13 response
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
g - SQL*Net data, R - outside acknowledged FIN,
R - UDP SUNRPC, r - inside acknowledged FIN, S - awaiting inside SYN,
s awaiting outside SYN, T SIP, t SIP transient, U up,
V - VPN orphan, W - WAAS,
X - inspected by service module

What can be determined about the connection status?

A. The output is showing normal activity to the inside 10.1.1.50 web server.



- B. Many HTTP connections to the 10.1.1.50 web server have successfully completed the three- way TCP handshake.
- C. Many embryonic connections are made from random sources to the 10.1.1.50 web server.
- D. The 10.1.1.50 host is triggering SYN flood attacks against random hosts on the outside.
- E. The 10.1.1.50 web server is terminating all the incoming HTTP connections.

Correct Answer: C

642-618 VCE Dumps

642-618 Practice Test

642-618 Study Guide



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.geekcert.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.



To ensure that you are spending on quality products, we provide 100% money back guarantee for <u>30 days</u>

Money Back Guarantee

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.

Any charges made through this site will appear as Global Simulators Limited. All trademarks are the property of their respective owners. Copyright © geekcert, All Rights Reserved.