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:

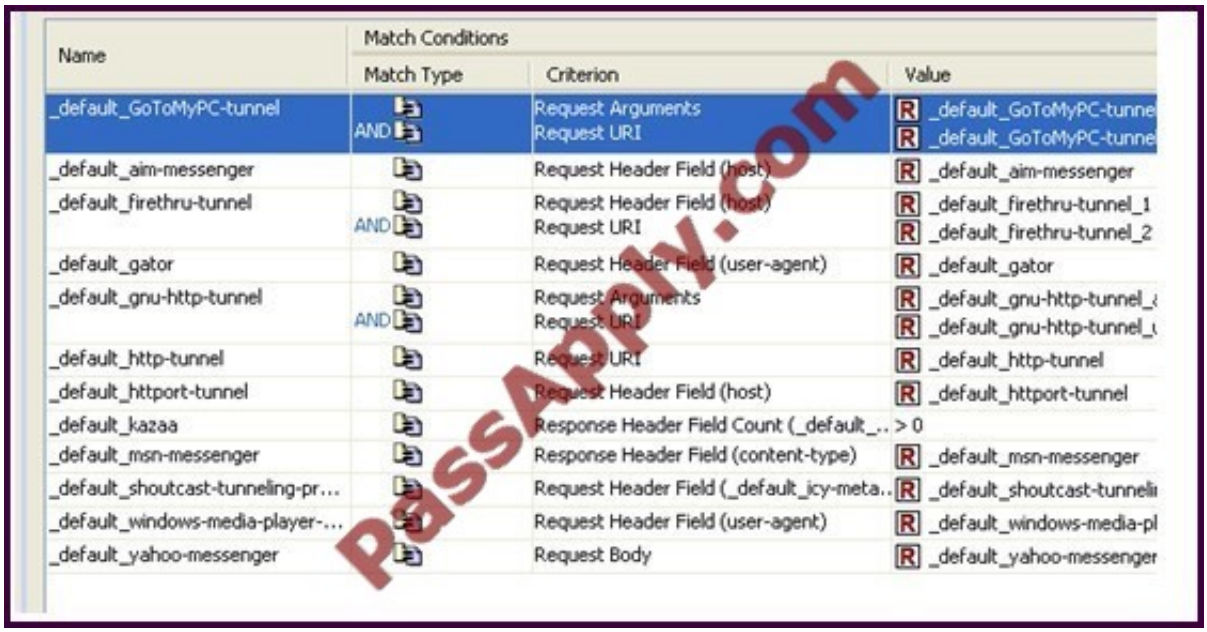
https://www.passapply.com/642-618.html

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.



Name	Match Conditions		
	Match Type	Criterion	Value
_default_GoToMyPC-tunnel	AND	Request Arguments Request URI	R _default_GoToMyPC-tunne R _default_GoToMyPC-tunne
_default_aim-messenger		Request Header Field (host)	R _default_aim-messenger
_default_firethru-tunnel	AND	Request Header Field (host) Request URI	R _default_firethru-tunnel_1 R _default_firethru-tunnel_2
_default_gator		Request Header Field (user-agent)	R _default_gator
_default_gnu-http-tunnel	AND	Request Arguments Request URI	R _default_gnu-http-tunnel_ R _default_gnu-http-tunnel_
_default_http-tunnel		Request URI	R _default_http-tunnel
_default_httport-tunnel		Request Header Field (host)	R _default_httport-tunnel
_default_kazaa		Response Header Field Count (_default_..	> 0
_default_msn-messenger		Response Header Field (content-type)	R _default_msn-messenger
_default_shoutcast-tunneling-pr...		Request Header Field (_default_icy-meta..	R _default_shoutcast-tunneli
_default_windows-media-player-...		Request Header Field (user-agent)	R _default_windows-media-pl
_default_yahoo-messenger		Request Body	R _default_yahoo-messenger

Which two statements about the class maps are true? (Choose two.)

A. These class maps are referenced within the global policy by default for HTTP inspection.

B. These class maps are all type inspect http class maps.

C. These class maps classify traffic using regular expressions.

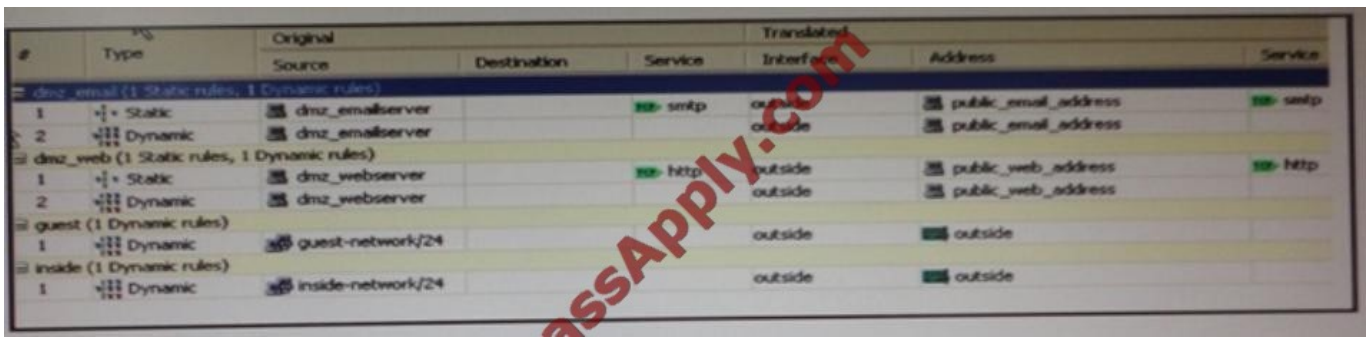
D. These class maps are Layer 3/4 class maps.

E. These class maps are used within the inspection_default class map for matching the default inspection traffic.

Correct Answer: BC

QUESTION 2

Refer to the Exhibit.



#	Type	Original Source	Original Destination	Original Service	Translated Interface	Translated Address	Translated Service
dmz_email (1 Static rules, 1 Dynamic rules)							
1	Static	dmz_emailserver		smtp	outside	public_email_address	smtp
2	Dynamic	dmz_emailserver			outside	public_email_address	
dmz_web (1 Static rules, 1 Dynamic rules)							
1	Static	dmz_webserver		http	outside	public_web_address	http
2	Dynamic	dmz_webserver			outside	public_web_address	
guest (1 Dynamic rules)							
1	Dynamic	guest-network/24			outside	outside	
inside (1 Dynamic rules)							
1	Dynamic	inside-network/24			outside	outside	

Which statement about the NAT/PAT configuration is true?

A. Dynamic PAT is used for any traffic that is sourced from the dmz_emailserver to the outside

B. Dynamic PAT is used for any traffic that is sourced from any host on the inside network to the outside

C. Static NAT is used for any traffic that is sourced from the dmz_emailserver to the outside

D. Static PAT is used for any traffic that is sourced from the dmz_emailserver to the outside

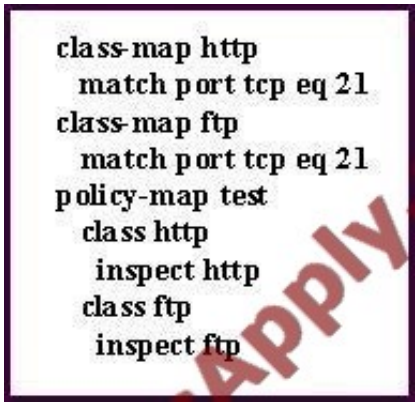
E. Dynamic NAT is used for any traffic that is sourced from the dmz_emailserver to the outside

F. Dynamic NAT is used for any traffic that is sourced from and host on the guest-network to the outside

Correct Answer: B

QUESTION 3

Refer to the exhibit.



Which statement about the policy map named test is true?

A. Only HTTP inspection will be applied to the TCP port 21 traffic.

B. Only FTP inspection will be applied to the TCP port 21 traffic.

C. both HTTP and FTP inspections will be applied to the TCP port 21 traffic.

D. No inspection will be applied to the TCP port 21 traffic, because the http class map configuration conflicts with the ftp class map.

E. All FTP traffic will be denied, because the FTP traffic will fail the HTTP inspection.

Correct Answer: B

QUESTION 4

By default, how does the Cisco ASA authenticate itself to the Cisco ASDM users?

A. The administrator validates the Cisco ASA by examining the factory built-in identity certificate thumbprint of the Cisco ASA.

B. The Cisco ASA automatically creates and uses a persistent self-signed X.509 certificate to authenticate itself to the administrator.

C. The Cisco ASA automatically creates a self-signed X.509 certificate on each reboot to authenticate itself to the administrator.

D. The Cisco ASA and the administrator use a mutual password to authenticate each other.

E. The Cisco ASA authenticates itself to the administrator using a one-time password.

Correct Answer: C

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a00808efb d2.shtml

QUESTION 5

With Cisco ASA active/active or active/standby stateful failover, which state information or table is not passed between the active and standby Cisco ASA by default?

A. NAT translation table

B. TCP connection states

C. UDP connection states

D. ARP table

E. HTTP connection table

Correct Answer: E

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/ha_overview.html#wp 1078922

Stateful Failover

When Stateful Failover is enabled, the active unit continually passes per-connection state information to the standby unit. After a failover occurs, the same connection information is available at the new active unit. Supported end-user applications are not required to reconnect to keep the same communication session.

Table 32-2 list the state information that is and is not passed to the standby unit when Stateful Failover is enabled.

Table 32-2 State Information

State Information Passed to Standby Unit	State Information Not Passed to Standby Unit
NAT translation table	The HTTP connection table (unless HTTP replication is enabled).
TCP connection states	The user authentication (uauth) table. Inspected protocols are subject to advanced TCP-state tracking, and the TCP state of these connections is not automatically replicated. While these connections are replicated to the standby unit, there is a best-effort attempt to re-establish a TCP state.
UDP connection states	The routing tables. After a failover occurs, some packets may be lost or routed out of the wrong interface (the default route) while the dynamic routing protocols rediscover routes.
The ARP table	State information for Security Service Modules.
The Layer 2 bridge table (when running in transparent firewall mode)	DHCP server address leases.
The HTTP connection states (if HTTP replication is enabled)	Stateful failover for phone proxy. When the active unit goes down, the call fails, media stops flowing, and the phone should unregister from the failed unit and reregister with the active unit. The call must be re-established.
The ISAKMP and IPSec SA table	—
GTP PDP connection database	—
SIP signalling sessions	—

The following WebVPN features are not supported with Stateful Failover:

- Smart Tunnels
- Port Forwarding
- Plugins
- Java Applets
- IPv6 clientless or Anyconnect sessions
- Citrix authentication (Citrix users must reauthenticate after failover)

QUESTION 6

Which Cisco ASA CLI command is used to enable HTTPS (Cisco ASDM) access from any inside host on the 10.1.16.0/20 subnet?

A. http 10.1.16.0 0.0.0.0 inside

B. http 10.1.16.0 0.0.15.255 inside

C. http 10.1.16.0 255.255.240.0 inside

D. http 10.1.16.0 255.255.255.255

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/mgaccess.html#wp104 Allowing HTTPS Access for ASDM

To use ASDM, you need to enable the HTTPS server, and allow HTTPS connections to the security appliance.

All of these tasks are completed if you use the setup command. This section describes how to manually configure ASDM access.

The security appliance allows a maximum of 5 concurrent ASDM instances per context, if available, with a maximum of 32 ASDM instances between all contexts.

Note WebVPN and ASDM administration cannot be enabled on the same interface. If you enable WebVPN on an interface, then that interface cannot be used for ASDM.

To configure ASDM access, follow these steps:

Step 1 To identify the IP addresses from which the security appliance accepts HTTPS connections, enter the following command for each address or subnet:

hostname(config)# http source_IP_address mask source_interface

Step 2 To enable the HTTPS server, enter the following command:

hostname(config)# http server enable

QUESTION 7

Which command option/keyword in Cisco ASA 8.3 NAT configurations makes the NAT policy interface independent?

A. interface

B. all

C. auto

D. global

E. any

Correct Answer: E

http://tunnelsup.com/2011/06/24/nat-for-cisco-asas-version-8-3/ Using the "any" interface in the NAT statement

ASA 8.3 introduces the "any" interface when configuring NAT. For instance if you have a system on the DMZ that you wish to NAT not only to the outside interface, but to any interface you can use this command: object network dmzwebserver host 192.168.1.23 nat (dmz,any) static 209.165.201.28 This makes it so users on the inside can web to 209.165.201.28 and if traffic is routed to the firewall it will NAT it to the real IP in the DMZ.

QUESTION 8

Which configuration step is the first to enable PIM-SM on the Cisco ASA appliance?

A. Configure the static RP IP address.

B. Enable IGMP forwarding on the required interface(s).

C. Add the required static mroute(s).

D. Enable multicast routing globally on the Cisco ASA appliance.

E. Configure the Cisco ASA appliance to join the required multicast groups.

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/route_multicast.html# wp1060775

Enabling Multicast Routing Enabling multicast routing lets the ASA forward multicast packets. Enabling multicast routing automatically enables PIM and IGMP on all interfaces.

To enable multicast routing, perform the following step:

Command	Purpose

`multicast-routing`
Example:
`hostname(config)# multicast-routing`
	This step enables multicast routing.
	The number of entries in the multicast routing tables are limited by the amount of RAM on the system.

QUESTION 9

On Cisco ASA Software Version 8.4.1 and later, when you configure the Cisco ASA appliance in transparent firewall mode, which configuration is mandatory?

A. NAT

B. static routes

C. ARP inspections

D. EtherType access-list

E. bridge group(s)

F. dynamic MAC address learning

Correct Answer: E

Command History

Release	Modification
7.0(1)	For routed mode, this command was changed from a global configuration command to an interface configuration mode command.
8.4(1)	For transparent mode, bridge groups were introduced. You now set the IP address for the BVI, and not globally.

Usage Guidelines

In single context routed firewall mode, each interface address must be on a unique subnet. In multiple context mode, if this interface is on a shared interface, then each IP address must be unique but on the same subnet. If the interface is unique, this IP address can be used by other contexts if desired.

A transparent firewall does not participate in IP routing. The only IP configuration required for the ASA is to set the BVI address. This address is required because the ASA uses this address as the source address for traffic originating on the ASA, such as system messages or communications with AAA servers. You can also use this address for remote management access. This address must be on the same subnet as the upstream and downstream routers. For multiple context mode, set the management IP address within each context. For models that include a Management interface, you can also set an IP address for this interface for management purposes.

The standby IP address must be on the same subnet as the main IP address.

Examples

The following example sets the IP addresses and standby addresses of two interfaces:

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```


QUESTION 10

On the Cisco ASA Software Version 8.4.1, which three parameters can be configured using the set connection command within a policy map? (Choose three.)

A. per-client TCP and/or UDP idle timeout

B. per-client TCP and/or UDP maximum session time

C. TCP sequence number randomization

D. maximum number of simultaneous embryonic connections

E. maximum number of simultaneous TCP and/or UDP connections

F. fragments reassembly options

Correct Answer: CDE

http://www.cisco.com/en/US/docs/security/asa/asa82/command/reference/s1.html#wp1424045

set connection

To specify connection limits within a policy map for a traffic class use the **set connection** command in class configuration mode. To remove these specifications, thereby allowing unlimited connections, use the **no** form of this command.

set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

no set connection {[**conn-max** *n*] [**embryonic-conn-max** *n*] [**per-client-embryonic-max** *n*] [**per-client-max** *n*] [**random-sequence-number** {**enable** | **disable**}]}

Syntax Description

conn-max *n*	Sets the maximum number of simultaneous TCP and/or UDP connections that are allowed, between 0 and 65535. The default is 0, which allows unlimited connections. For example, if two servers are configured to allow simultaneous TCP and/or UDP connections, the connection limit is applied to each configured server separately. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for the entire class. In this case, one stack host can consume all the connections and leave none of the rest of the hosts matched in the access list under the class.
embryonic-conn-max *n*	Sets the maximum number of simultaneous embryonic connections allowed, between 0 and 65535. The default is 0, which allows unlimited connections.
per-client-embryonic-max *n*	Sets the maximum number of simultaneous embryonic connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the adaptive security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the embryonic limit is applied per-host, and not the cumulative embryonic connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps.
per-client-max *n*	Sets the maximum number of simultaneous connections allowed per client, between 0 and 65535. A client is defined as the host that sends the initial packet of a connection (that builds the new connection) through the adaptive security appliance. If an **access-list** is used with a **class-map** to match traffic for this feature, the connection limit is applied per-host, and not the cumulative connections of all clients that match the access list. The default is 0, which allows unlimited connections. This keyword is not available for management class maps. When configured under a class, this keyword restricts the maximum number of simultaneous connections that are allowed for each host that is matched through an access list under the class.
random-sequence-number {**enable** | **disable**}	Enables or disables TCP sequence number randomization. This keyword is not available for management class maps. See the "Usage Guidelines" section for more information.

QUESTION 11

Which configuration step (if any) is necessary to enable FTP inspection on TCP port 2121?

A. None. FTP inspection is enabled by default using the global policy.

B. Create a new class map to match TCP port 2121, then edit the global policy to inspect FTP for traffic matched by the new class map.

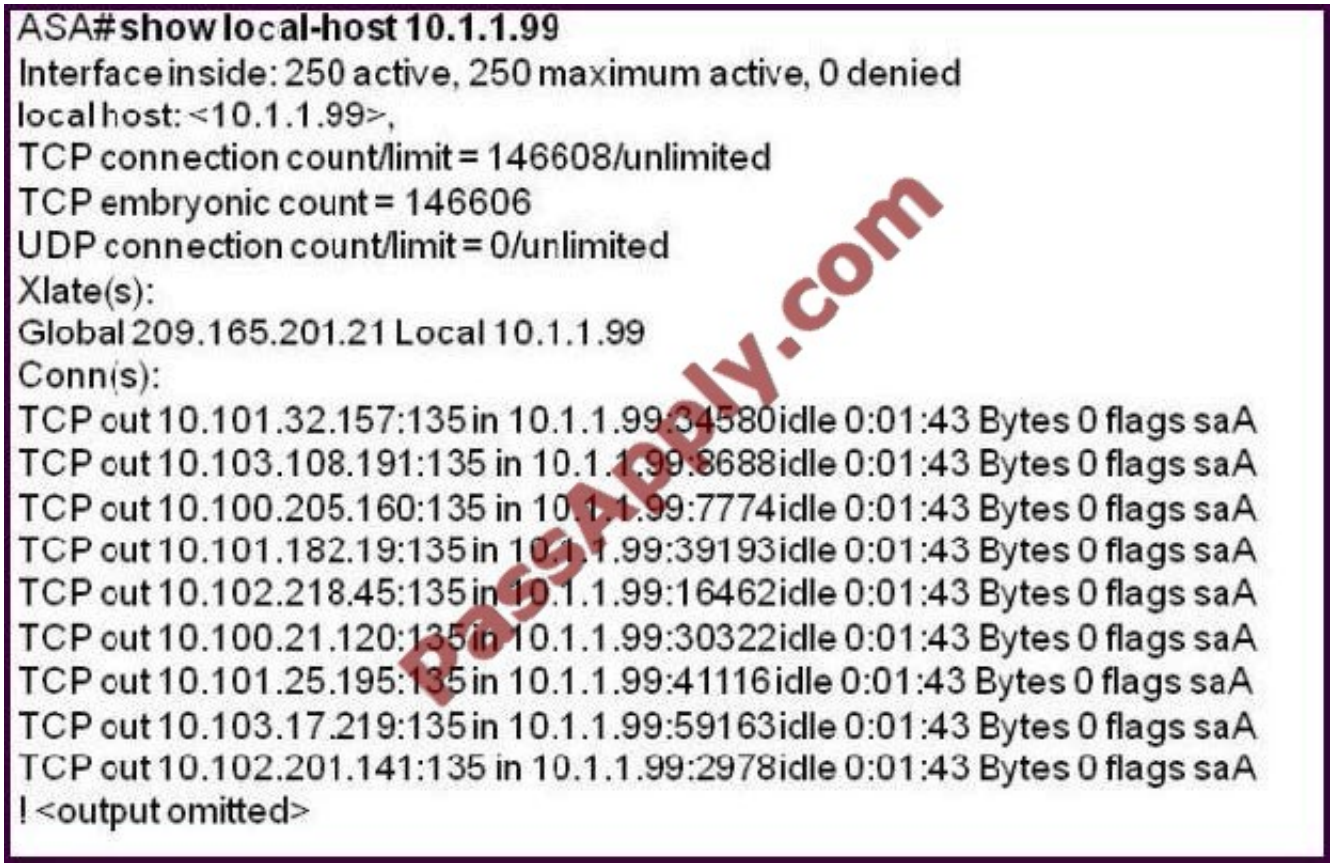
C. Edit default-inspection-traffic to match FTP on port 2121.

D. Add a new traffic class using the match protocol FTP option within the inspect_default class map.

Correct Answer: B

QUESTION 12

Refer to the exhibit.



What is a reasonable conclusion?

A. The maximum number of TCP connections that the 10.1.1.99 host can establish will be 146608.

B. All the connections from the 10.1.1.99 have completed the TCP three-way handshake.

C. The 10.1.1.99 hosts are generating a vast number of outgoing connections, probably due to a virus.

D. The 10.1.1.99 host on the inside is under a SYN flood attack.

E. The 10.1.1.99 host operations on the inside look normal.

Correct Answer: C

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 t3-response
k - Skinny media, M - SMTP data, m - SIP media, n - GUP
O - outbound data, P - inside back connection, p - Phone-proxy TFTP connection,
q - 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

[642-618 VCE Dumps](#) [642-618 Exam Questions](#) [642-618 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.passapply.com/allproducts

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket: