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.pass4itsure.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

By default, which access rule is applied inbound to the inside interface?

A. All IP traffic is denied.

B. All IP traffic is permitted.

C. All IP traffic sourced from any source to any less secure network destinations is permitted.

D. All IP traffic sourced from any source to any more secure network destinations is permitted

Correct Answer: C

http://www.cisco.com/en/US/docs/security/asa/asa84/configuration/guide/access_rules.html#wp 1083496

Implicit Permits

For routed mode, the following types of traffic are allowed through by default:

-IPv4 traffic from a higher security interface to a lower security interface.

-IPv6 traffic from a higher security interface to a lower security interface. Note These defaults might not be true if you have configured a global access rule. For transparent mode, the following types of traffic are allowed through by default:

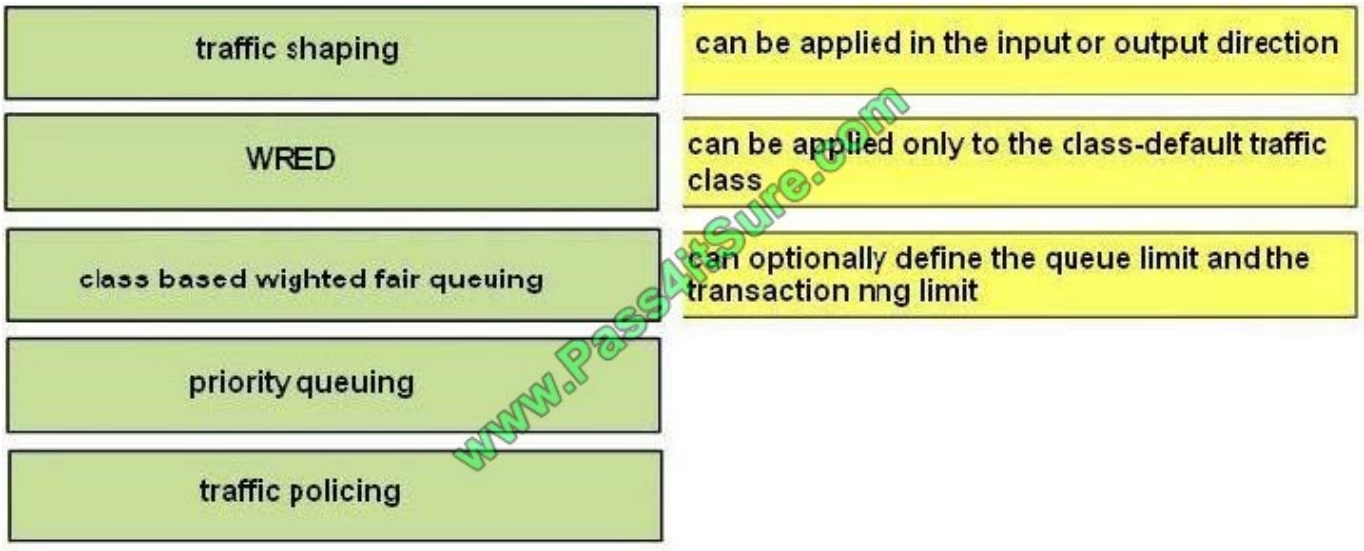
-IPv4 traffic from a higher security interface to a lower security interface. -IPv6 traffic from a higher security interface to a lower security interface.

-ARPs in both directions

QUESTION 2

Click and drag the supported ASA QoS option on the left to the correct description on the right. (Some of the options on the left are not used)

Select and Place:



Correct Answer:

QUESTION 3

Which two statements about Cisco ASA 8.2 NAT configurations are true? (Choose two.)

A. NAT operations can be implemented using the NAT, global, and static commands.

B. If nat-control is enabled and a connection does not need a translation, then an identity NAT configuration is required.

C. NAT configurations can use the any keyword as the input or output interface definition.

D. The NAT table is read and processed from the top down until a translation rule is matched.

E. Auto NAT links the translation to a network object.

Correct Answer: AB

http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008046f3 1a.shtml#IN1

QUESTION 4

The Cisco ASA is configured in multiple mode and the security contexts share the same outside physical interface.

Which two packet classification methods can be used by the Cisco ASA to determine which security context to forward the incoming traffic from the outside interface? (Choose two.)

A. unique interface IP address

B. unique interface MAC address

C. routing table lookup

D. MAC address table lookup

E. unique global mapped IP addresses

Correct Answer: BE

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

Unique Interfaces

If only one context is associated with the ingress interface, the ASA classifies the packet into that context. In transparent firewall mode, unique interfaces for contexts are required, so this method is used to classify packets at all times.

Unique MAC Addresses

If multiple contexts share an interface, then the classifier uses the interface MAC address. The ASA lets you assign a different MAC address in each context to the same shared interface, whether it is a shared physical interface or a shared

subinterface. By default, shared interfaces do not have unique MAC addresses; the interface uses the physical interface burned-in MAC address in every context. An upstream router cannot route directly to a context without unique MAC

addresses. You can set the MAC addresses manually when you configure each interface (see the "Configuring the MAC Address" section), or you can automatically generate MAC addresses (see the "Automatically Assigning MAC

Addresses to Context Interfaces" section).

NAT Configuration

If you do not have unique MAC addresses, then the classifier intercepts the packet and performs a destination IP address lookup. All other fields are ignored; only the destination IP address is used. To use the destination address for

classification, the classifier must have knowledge about the subnets located behind each security context. The classifier relies on the NAT configuration to determine the subnets in each context. The classifier matches the destination IP

address to either a static command or a global command. In the case of the global command, the classifier does not need a matching nat command or an active NAT session to classify the packet. Whether the packet can communicate with

the destination IP address after classification depends on how you configure NAT and NAT control.

For example, the classifier gains knowledge about subnets 10.10.10.0, 10.20.10.0 and 10.30.10.0 when the context administrators configure static commands in

each context:

-Context A:

static (inside,shared) 10.10.10.0 10.10.10.0 netmask 255.255.255.0

-Context B:

static (inside,shared) 10.20.10.0 10.20.10.0 netmask 255.255.255.0

QUESTION 5

Which four unicast or multicast routing protocols are supported by the Cisco ASA appliance? (Choose four.)

A. RIP (v1 and v2)

B. OSPF

C. ISIS

D. BGP

E. EIGRP

F. Bidirectional PIM

G. MOSPF

H. PIM dense mode

Correct Answer: ABEF

http://www.cisco.com/en/US/docs/security/asa/asa84/asdm64/configuration_guide/route_overvie w.html#wp1125708

-Enhanced Interior Gateway Routing Protocol (EIGRP)

Enhanced IGRP provides compatibility and seamless interoperation with IGRP routers. An automaticredistribution mechanism allows IGRP routes to be imported into Enhanced IGRP, and vice versa, so it is possible to add Enhanced IGRP

gradually into an existing IGRP network. For more infomation on configuring EIGRP, see the chapter `Configuring EIGRP\\'.

-Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is a routing protocol developed for Internet Protocol (IP) networks by the interior gateway protocol (IGP) working group of the Internet Engineering Task Force (IETF). OSPF uses a linkstate algorithm in order

to build and calculate the shortest path to all known destinations. Each router in an OSPF area contains an identical link-

state database, which is a list of each of the router usable interfaces and reachable neighbors

For more infomation on configuring OSPF, see the chapter `Configuring OSPF\\'. -Routing Information Protocol The Routing Information Protocol (RIP) is a distance-vector protocol that uses hop count as its metric. RIP is widely used for

routing traffic in the global Internet and is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system.

For more infomation on configuring RIP, see the chapter `Configuring RIP\\'.
http://www.cisco.com/en/US/docs/security/asa/asa81/config/guide/multicst.html#wp1060775

Multicast Routing Overview The adaptive security appliance supports both stub multicast routing and PIM multicast routing. However, you cannot configure both concurrently on a single adaptive security appliance.

Stub multicast routing provides dynamic host registration and facilitates multicast routing. When configured for stub multicast routing, the adaptive security appliance acts as an IGMP proxy agent. Instead of fully participating in multicast

routing, the adaptive security appliance forwards IGMP messages to an upstream multicast router, which sets up delivery of the multicast data. When configured for stub multicast routing, the adaptive security appliance cannot be configured

for PIM.

The adaptive security appliance supports both PIM-SM and bi-directional PIM. PIM-SM is a multicast routing protocol that uses the underlying unicast routing information base or a separate multicast-capable routing information base. It builds

unidirectional shared trees rooted at a single Rendezvous Point per multicast group and optionally creates shortest-path trees per multicast source.

Bi-directional PIM is a variant of PIM-SM that builds bi-directional shared trees connecting multicast sources and receivers. Bi-directional trees are built using a DF election process operating on each link of the multicast topology. With the

assistance of the DF, multicast data is forwarded from sources to the Rendezvous Point, and therefore along the shared tree to receivers, without requiring source-specific state. The DF election takes place during Rendezvous Point

discovery and provides a default route to the Rendezvous Point.

QUESTION 6

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 7

Which access rule is disabled automatically after the global access list has been defined and applied?

A. the implicit global deny ip any any access rule

B. the implicit interface access rule that permits all IP traffic from high security level to low security level interfaces

C. the implicit global access rule that permits all IP traffic from high security level to low security level interfaces

D. the implicit deny ip any any rule on the global and interface access lists

E. the implicit permit all IP traffic from high security level to low security level access rule on the global and interface access lists

Correct Answer: B

http://www.cisco.com/en/US/docs/security/security_management/cisco_security_manager/security_manager/4.3/user/guide/fwaccess.html

Understanding Device Specific Access Rule Behavior

If you do not create an access rule policy, the following is the default behavior based on the type of device, and what happens when you create an access rule:

-IOS devices--Permit all traffic through an interface.

When you create an access rule permitting source A to destination B without configuring TCP/UDP inspection on the inspection rule table, or configuring the established advanced option on the rule, the device permits any packet from A to B.

However, for any returning packet from B to A, the packet is not allowed, unless there is a corresponding access rule permitting that packet. If you configure TCP/UDP inspection on the traffic the inspection rule table, a rule permitting B to A is

not needed in the access rule, as any returning packet from B to A automatically passes the device.

-ASA and PIX devices--Permit traffic from a higher-security interface to a lower-security interface. Otherwise, all traffic is denied.

If an access rule allows TCP/UDP traffic in one direction, the appliance automatically allows return traffic (you do not need to configure a corresponding rule for the return traffic), except for ICMP traffic, which does require a return rule (where

you permit the reverse source and destination), or you must create an inspection rule for ICMP.

-FWSM devices--Deny all traffic entering an interface, permit all traffic leaving an interface. You must configure access rules to allow any traffic to enter the device.

QUESTION 8

On the Cisco ASA, tcp-map can be applied to a traffic class using which MPF CLI configuration command?

A. inspect

B. sysopt connection

C. tcp-options

D. parameters

E. set connection advanced-options

Correct Answer: E

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

QUESTION 9

Which two statements about Cisco ASA redundant interface configuration are true? (Choose two.)

A. Each redundant interface can have up to four physical interfaces as its member.

B. When the standby interface becomes active, the Cisco ASA sends gratuitous ARP out on the standby interface.

C. Interface duplex and speed configurations are configured under the redundant interface.

D. Redundant interfaces use MAC address-based load balancing to load share traffic across multiple physical interfaces.

E. Each Cisco ASA supports up to eight redundant interfaces.

Correct Answer: BE

Configuring a Redundant Interface A logical redundant interface pairs an active and a standby physical interface. When the active interface fails, the standby interface becomes active and starts passing traffic. You can configure a redundant interface to increase the security appliance reliability. This feature is separate from device-level failover, but you can configure redundant interfaces as well as failover if desired.

You can configure up to 8 redundant interface pairs.

In Active/Standby failover, the active device uses the primary unit\\'s MAC addresses. In the event of a failover, the secondary Cisco ASA becomes active and takes over the primary unit\\'s MAC addresses, while the active device (now standby) takes over the standby unit\\'s MAC addresses. Once the standby Cisco ASA becomes active, it sends out a gratuitous ARP on the network.

A gratuitous ARP is an ARP request that the Cisco ASA sends out on the Ethernet networks with the source and destination IP addresses of the active IP addresses. The destination MAC address is the Ethernet broadcast address, i.e., ffff.ffff.ffff. All devices on the

Ethernet segment process this broadcast frame and update their ARP table with this information. Using gratuitous ARP, the Layer 2 devices, including bridges and switches, also update the Content Addressable Memory (CAM) table with the MAC address and the updated switch port information.

Using a virtual MAC address is recommended to avoid network disruptions. When a secondary Cisco ASA boots up before the primary Cisco ASA, it uses its physical MAC addresses as active Layer 2 addresses.

However, when the primary Cisco ASA boots up, the secondary swaps the MAC addresses and uses the primary Cisco ASA\\'s physical MAC addresses as active.

With the virtual MAC address, Cisco ASA do not need to swap the MAC address.

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.

The state information passed to the standby unit includes these: The NAT translation table The TCP connection states The UDP connection states The ARP table The Layer 2 bridge table (when it runs in the transparent firewall mode) The HTTP connection states (if HTTP replication is enabled) The ISAKMP and IPSec SA table The GTP PDP connection database The information that is not passed to the standby unit when stateful failover is enabled includes these:

The HTTP connection table (unless HTTP replication is enabled) The user authentication (uauth) table

The routing tables State information for security service modules Note: If failover occurs within an active Cisco IP SoftPhone session, the call remains active because the call session state information is replicated to the standby unit. When the call is terminated, the IP SoftPhone client loses connection with the Call Manager. This occurs because there is no session information for the CTIQBE hang-up message on the standby unit. When the IP SoftPhone client does not receive a response back from the Call Manager within a certain time period, it considers the Call Manager unreachable and unregisters itself.

QUESTION 10

Which Cisco ASA configuration is used to configure the TCP intercept feature?

A. a TCP map

B. an access list

C. the established command

D. the set connection command with the embryonic-conn-max option

E. a type inspect policy map

Correct Answer: D

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/conns_connlimits.html #wp1080734

QUESTION 11

The Cisco ASA must support dynamic routing and terminating VPN traffic. Which three Cisco ASA options will not support these requirements? (Choose three.)

A. transparent mode

B. multiple context mode

C. active/standby failover mode

D. active/active failover mode

E. routed mode

F. no NAT-control

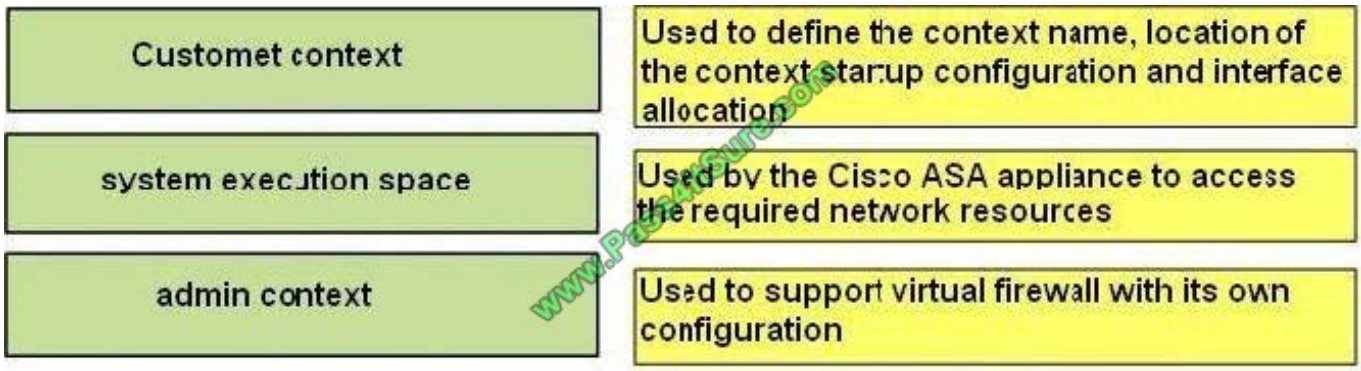
Correct Answer: ABD

Dynamic routing (OSPF and RIP (in passive mode)) is supported by routed firewall. Dynamic routing is NOT supported in Transparent UNLESS you can allow dynamic routing protocols through the ASA using an extended access list Dynamic routing is NOT supported in Multiple context mode

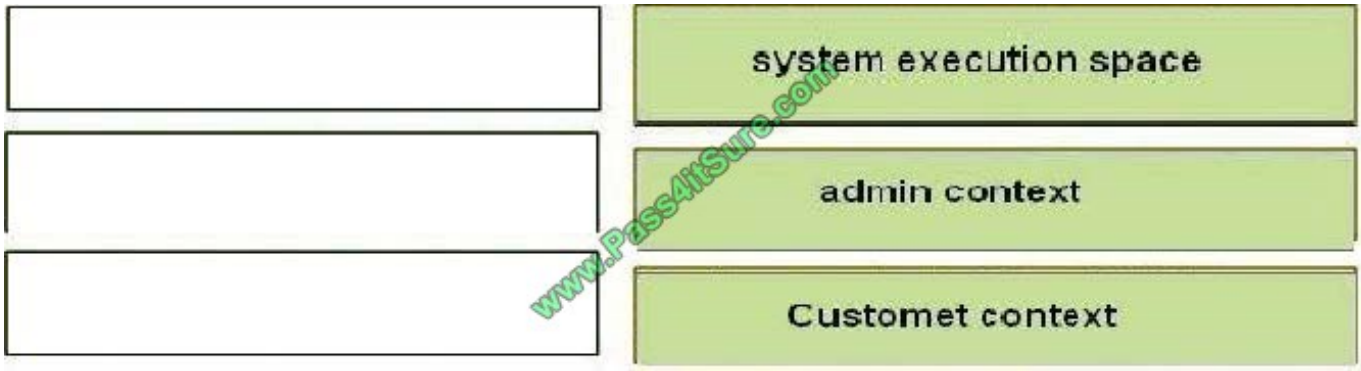
QUESTION 12

Drag the Cisco ASR modes from the left to the correct description on the right.

Select and Place:



Correct Answer:



Systems Execution SpaceUsed to define the context name, location of the context startup configuration and interface allocation Admin ContextUsed by the Cisco ASA appliance to access the required network resources Customer contextUsed to support virtual firewall with its own configuration Context Configurations The security appliance includes a configuration for each context that identifies the security policy, interfaces, and almost all the options you can configure on a standalone device. You can store context configurations on the internal Flash memory or the external Flash memory card, or you can download them from a TFTP, FTP, or HTTP(S) server.

System Configuration The system administrator adds and manages contexts by configuring each context configuration location, allocated interfaces, and other context operating parameters in the system configuration, which, like a single mode configuration, is the startup configuration. The system configuration identifies basic settings for the security

appliance. The system configuration does not include any network interfaces or network settings for itself; rather, when the system needs to access network resources (such as downloading the contexts from the server), it uses one of the contexts that is designated as the admin context. The system configuration does include a specialized failover interface for failover traffic only.

Admin Context Configuration The admin context is just like any other context, except that when a user logs in to the admin context, then that user has system administrator rights and can access the system and all other contexts. The admin context is not restricted in any way, and can be used as a regular context. However, because logging into the admin context grants you administrator privileges over all contexts, you might need to restrict access to the admin context to appropriate users. The admin context must reside on Flash memory, and not remotely.

Latest 642-618 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 !

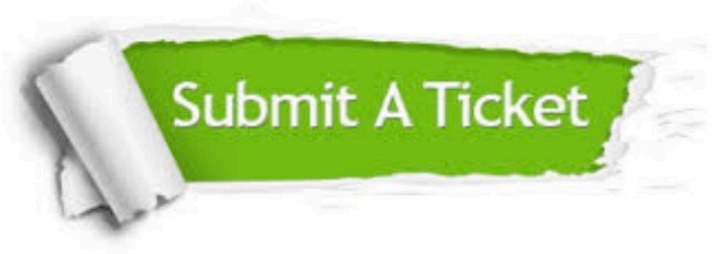
100% Guaranteed Success
100% Money Back Guarantee
365 Days Free Update
Instant Download After Purchase
24x7 Customer Support
Average 99.9% Success Rate
More than 800,000 Satisfied Customers Worldwide
Multi-Platform capabilities - Windows, Mac, Android, iPhone, iPod, iPad, Kindle

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.pass4itsure.com/allproducts

Need Help

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



Any charges made through this site will appear as Global Simulators Limited.
All trademarks are the property of their respective owners.
Copyright © pass4itsure, All Rights Reserved.