CCNA Cyber Ops (Version 1.1) – Chapter 5 Exam Answers Full

itexamanswers.net/ccna-cyber-ops-chapter-5-exam-answers-full.html

May 13, 2019

How to find: Press **"Ctrl + F"** in the browser and fill in whatever wording is in the question to find that question/answer. If the question is not here, find it in **Questions Bank**.

NOTE: If you have the new question on this test, please comment Question and Multiple-Choice list in form below this article. We will update answers for you in the shortest time. Thank you! We truly value your contribution to the website.

1. What specialized network device is responsible for enforcing access control policies between networks?

- Bridge
- Switch
- **Firewall**
- IDS

C. Firewalls are used to permit or block traffic between networks according to access control policies.

2. What information does an Ethernet switch examine and use to build its address table?

- Source IP address
- Destination IP address
- **Source MAC address**
- Destination MAC address

C. An Ethernet switch examines the source MAC address of an incoming frame. If the source MAC address is not in the MAC address table, the switch will add it to the table with the associated ingress Ethernet port.

3. Which device is an intermediary device?

- Smart device
- PC
- Server
- **Firewall**

D. An intermediary device sends network messages toward a final destination. Examples of intermediary devices include a firewall, router, switch, multilayer switch, and wireless router.

4. Which statement describes a difference between RADIUS and TACACS+?

- RADIUS uses TCP, whereas TACACS+ uses UDP.
- RADIUS is supported by the Cisco Secure ACS software, whereas TACACS+ is not.
- **RADIUS encrypts only the password, whereas TACACS+ encrypts all communication.**
- RADIUS separates authentication and authorization, whereas TACACS+ combines them as one process.

C. TACACS+ uses TCP, encrypts the entire packet (not just the password), and separates authentication and authorization into two distinct processes. Both protocols are supported by the Cisco Secure ACS software.

5. Which wireless parameter refers to the frequency bands used to transmit data to a wireless access point?

- SSID
- Security mode
- Scanning mode
- **Channel settings**

D. An access point can be manually set to a specific frequency band or channel in order to avoid interference with other wireless devices in the area.

6. What specialized network device uses signatures to detect patterns in network traffic?

- Bridges
- Switches
- **IDS**
- Firewalls

C. Intrusion detection systems (IDSs) use a set of rules, referred to as signatures, to identify malicious traffic on the network.

7. What type of physical topology can be created by connecting all Ethernet cables to a central device?

- **Star**
- Bus
- Ring
- Mesh

A. Devices connected to the Ethernet star topology connect to either a hub or a switch.

8. Which network service synchronizes the time across all devices on the network?

- NetFlow
- Syslog
- **NTP**
- SNMP

C. There are two methods that can be used to set date and time settings on network devices. Manual configuration and automatically using the Network Time Protocol (NTP). NTP keeps the time across all devices synchronized by using a hierarchical system of sources.

9. Which network service allows administrators to monitor and manage network devices?

- NTP
- **SNMP**
- Syslog
- NetFlow

B. SNMP is an application layer protocol that allows administrators to manage and monitor devices on the network such as routers, switches, and servers.

10. What are two types of addresses found on network end devices? (Choose two.)

- UDP
- return
- **IP**
- TCP
- **MAC**

Intermediary devices use two types of addresses when sending messages to the final destination device, MAC and IP addresses. TCP and UDP are protocols used at Layer 4 to identify what port numbers are being used on the source and destination devices. A return address is used when mailing a letter, not in networking.

11. Which OSI layer header is rewritten with new addressing information by a router when forwarding between LAN segments?

- **Layer 2**
- Layer 3
- Layer 4

- Layer 7

When a router forwards traffic between LAN segments it encapsulates the Layer 2 frame to determine the Layer 3 path. Once the Layer 3 path is determined, the router encapsulates the Layer 3 packet in a new Layer 2 frame with new Layer 2 addressing infomation for the destination LAN segment.

12. Which protocol provides authentication, integrity, and confidentiality services and is a type of VPN?

- MD5
- AES
- ESP
- **IPsec**

IPsec services allow for authentication, integrity, access control, and confidentiality. With IPsec, the information exchanged between remote sites can be encrypted and verified. Both remote-access and site-to-site VPNs can be deployed using IPsec.

13. What are two uses of an access control list? (Choose two.)

- **ACLs can control which areas a host can access on a network.**
- **ACLs provide a basic level of security for network access.**
- Standard ACLs can restrict access to specific applications and ports.
- ACLs can permit or deny traffic based upon the MAC address originating on the router.
- ACLs assist the router in determining the best path to a destination.

ACLs can be used for the following:Limit network traffic in order to provide adequate network performance
Restrict the delivery of routing updates
Provide a basic level of security
Filter traffic based on the type of traffic being sent
Filter traffic based on IP addressing

14. Which protocol or service is used to automatically synchronize the software clocks on Cisco routers?

- SNMP
- **NTP**
- DHCP
- DNS

Network Time Protocol (NTP) is used to allow network devices to synchronize their time settings with a centralized time server. DHCP (Dynamic Host Configuration Protocol) is a protocol which assigns IP addresses to hosts. DNS (Domain Name Service) is a service which

resolves host names to IP addresses. SNMP (Simple Network Management Protocol) is a protocol which allows administrators to manage network nodes.

15. What is the only attribute used by standard access control lists to identify traffic?

- source MAC address
- protocol type
- **source IP address**
- source TCP port

Standard access control lists can only identify traffic based on the source IPv4 address in the protocol header.

16. Which wireless parameter is used by an access point to broadcast frames that include the SSID?

- **passive mode**
- security mode
- channel setting
- active mode

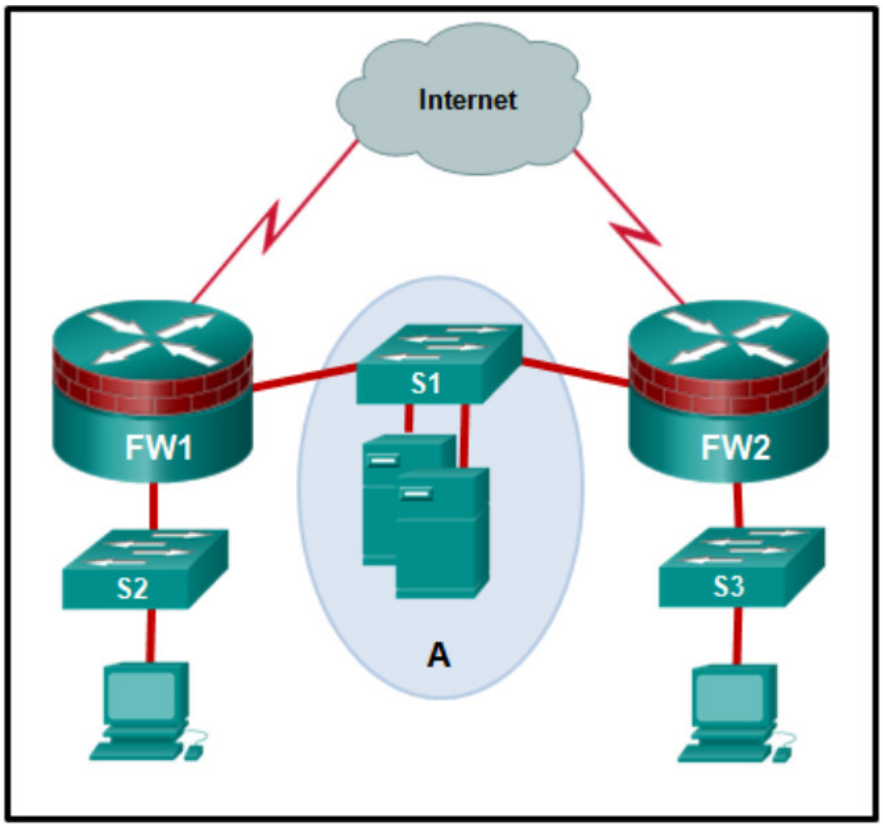
The two scanning or probing modes an access point can be placed into are passive or active. In passive mode, the AP advertises the SSID, supported standards, and security settings in broadcast beacon frames. In active mode, the wireless client must be manually configured for the same wireless parameters as the AP has configured.

17. A Cisco router is running IOS 15. What are the two routing table entry types that will be added when a network administrator brings an interface up and assigns an IP address to the interface? (Choose two.)

- route that is learned via OSPF
- route that is learned via EIGRP
- route that is manually entered by a network administrator
- **directly connected interface**
- **local route interface**

A local route interface routing table entry is found when a router runs IOS 15 or higher or if IPv6 routing is enabled. Whenever an interface is addressed and enabled (made active), a directly connected interface is automatically shown in the routing table.

18. Refer to the exhibit. The network "A" contains multiple corporate servers that are accessed by hosts from the Internet for information about the corporation. What term is used to describe the network marked as "A"?



- perimeter security boundary
- internal network
- **DMZ**
- untrusted network

A demilitarized zone or DMZ is a network area protected by one or more firewalls. The DMZ typically contains servers that are commonly accessed by external users. A web server is commonly contained in a DMZ.

19. What is the role of an IPS?

- **to detect patterns of malicious traffic by the use of signature files**
- to filter traffic based on defined rules and connection context
- to filter traffic based on Layer 7 information
- to enforce access control policies based on packet content

For detecting malicious activity, an IPS uses a set of rules called signatures to detect patterns in network traffic.

20. Which two features are included by both TACACS+ and RADIUS protocols? (Choose two.)

- SIP support
- **password encryption**

- 802.1X support
- separate authentication and authorization processes
- **utilization of transport layer protocols**

Both TACACS+ and RADIUS support password encryption (TACACS+ encrypts all communication) and use Layer 4 protocol (TACACS+ uses TCP and RADIUS uses UDP). TACACS+ supports separation of authentication and authorization processes, while RADIUS combines authentication and authorization as one process. RADIUS supports remote access technology, such as 802.1x and SIP; TACACS+ does not.

21. What does the TACACS+ protocol provide in a AAA deployment?

- AAA connectivity via UDP
- compatibility with previous TACACS protocols
- **authorization on a per-user or per-group basis**
- password encryption without encrypting the packet

TACACS+ utilizes TCP port 49, provides authorization on a per-user or per-group basis, encrypts the entire packet, and does not provide compatibility with previous TACACS protocols.

22. Which parameter is commonly used to identify a wireless network name when a home wireless AP is being configured?

- ESS
- **SSID**
- ad hoc
- BESS

The SSID is used to name a wireless network. This parameter is required in order for a wireless client to attach to a wireless AP.

23. What information within a data packet does a router use to make forwarding decisions?

- the destination service requested
- **the destination IP address**
- the destination host name
- the destination MAC address

A Layer 3 device like a router uses a Layer 3 destination IP address to make a forwarding decision.

24. Which protocol creates a virtual point-to-point connection to tunnel unencrypted traffic between Cisco routers from a variety of protocols?

- **GRE**
- IPsec
- OSPF
- IKE

Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco that encapsulates multiprotocol traffic between remote Cisco routers. GRE does not encrypt data. OSPF is a open source routing protocol. IPsec is a suite of protocols that allow for the exchange of information that can be encrypted and verified. Internet Key Exchange (IKE) is a key management standard used with IPsec.

25. Which two statements are true about NTP servers in an enterprise network? (Choose two.)

- **NTP servers at stratum 1 are directly connected to an authoritative time source.**
- **NTP servers ensure an accurate time stamp on logging and debugging information.**
- There can only be one NTP server on an enterprise network.
- All NTP servers synchronize directly to a stratum 1 time source.
- NTP servers control the mean time between failures (MTBF) for key network devices.

Network Time Protocol (NTP) is used to synchronize the time across all devices on the network to make sure accurate timestamping on devices for managing, securing and troubleshooting. NTP networks use a hierarchical system of time sources. Each level in this hierarchical system is called a stratum. The stratum 1 devices are directly connected to the authoritative time sources.

26. What is true concerning physical and logical topologies?

- Physical topologies display the IP addressing scheme of each network.
- **Logical topologies refer to how a network transfers data between devices.**
- The logical topology is always the same as the physical topology.
- Physical topologies are concerned with how a network transfers frames.

Physical topologies show the physical interconnection of devices. Logical topologies show the way the network will transfer data between connected nodes.

27. Which layer of the hierarchical design model is a control boundary between the other layers?

- access
- network
- **distribution**

- core

The three design layers from lowest to highest are access, distribution, and core. The distribution layer commonly provides policy-based connectivity which permits or denies traffic based on predefined parameters. The distribution layer also acts as a control boundary between the access and core layers.

28. Which protocol or service allows network administrators to receive system messages that are provided by network devices?

- NTP
- NetFlow
- SNMP
- **syslog**

Cisco developed NetFlow for the purpose of gathering statistics on packets flowing through Cisco routers and multilayer switches. SNMP can be used to collect and store information about a device. Syslog is used to access and store system messages.
NTP is used to allow network devices to synchronize time settings.

29. What is a function of a proxy firewall?

- uses signatures to detect patterns in network traffic
- **connects to remote servers on behalf of clients**
- drops or forwards traffic based on packet header information
- filters IP traffic between bridged interfaces

Proxy firewalls filter traffic through the application layer of the TPC/IP model and shield client information by connecting to remote servers on behalf of clients.

30. What is the function of the distribution layer of the three-layer network design model?

- **aggregating access layer connections**
- providing high speed connection to the network edge
- providing secure access to the Internet
- providing direct access to the network

The function of the distribution layer is to provide connectivity to services and to aggregate the access layer connections

31.Which LAN topology requires a central intermediate device to connect end devices?

- **star**

- ring
- bus
- mesh

In a star network topology end devices are connected to a central intermediate device such as a hub or a switch.

32. Which device can control and manage a large number of corporate APs?

- switch
- **WLC**
- router
- LWAP

A wireless LAN controller (WLC) can be configured to manage multiple lightweight access points (LWAPs). On the WLC, a network administrator can configure SSIDs, security, IP addressing, and other wireless network parameters in a centralized management environment.

33. For which discovery mode will an AP generate the most traffic on a WLAN?

- active mode
- mixed mode
- **passive mode**
- open mode

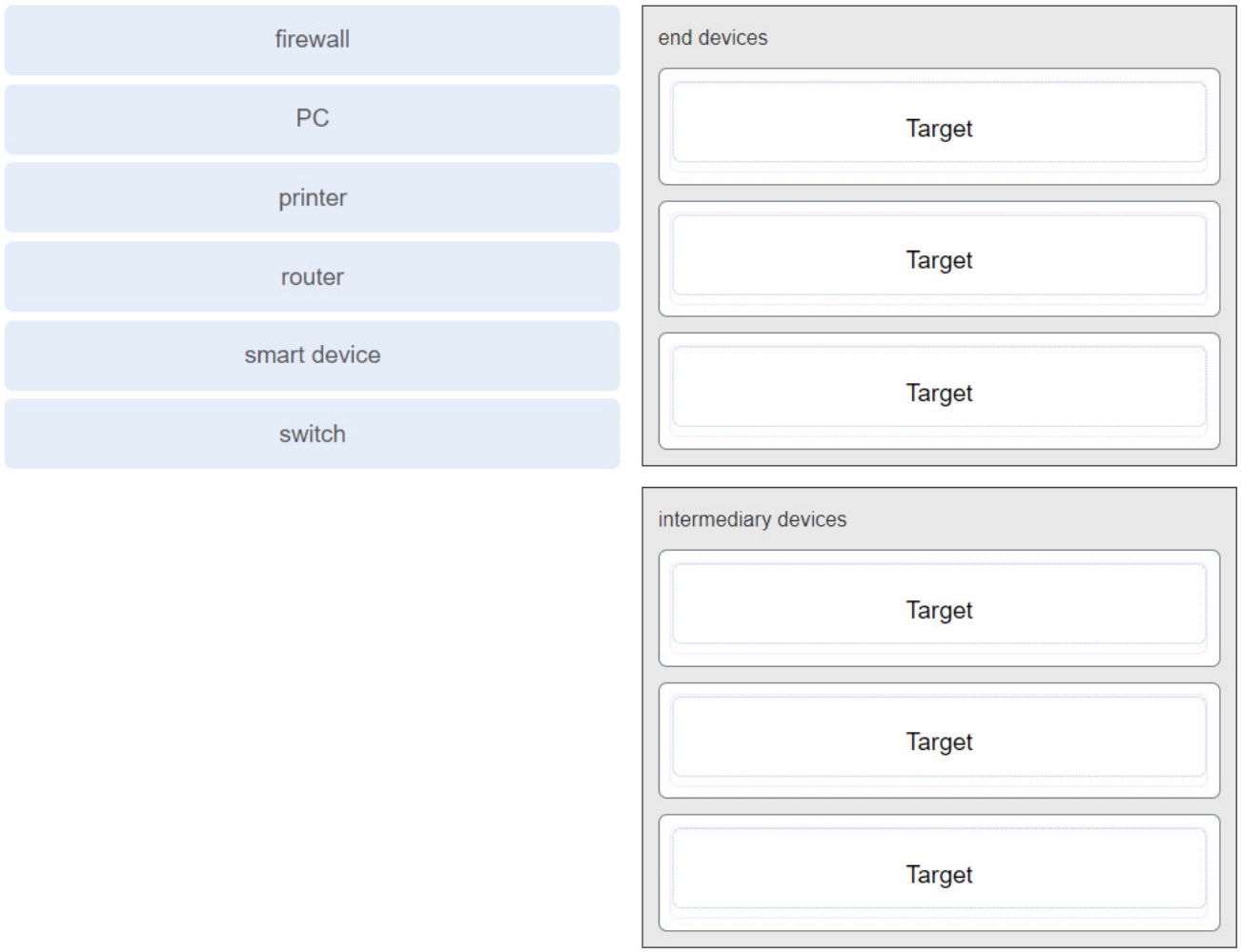
The two discovery modes are passive and active. When operating in passive mode, an AP will generate more traffic as it continually broadcasts beacon frames to potential clients. In active mode, the client initiates the discovery process instead of the AP. Mixed mode refers to network mode settings, and open mode refers to security parameter settings.

34. What is a feature of the TACACS+ protocol?

- It utilizes UDP to provide more efficient packet transfer.
- It hides passwords during transmission using PAP and sends the rest of the packet in plaintext.
- **It encrypts the entire body of the packet for more secure communications.**
- It combines authentication and authorization as one process.

TACACS+ has the following features:separates authentication and authorization
encrypts all communication
uses TCP port 49

35. Match each device to a category.


firewall
PC
printer
router
smart device
switch
end devices
Target
Target
Target
intermediary devices
Target
Target
Target

Answer

36. Match the destination network routing table entry type with a defintion.

directly connected interface

dynamic route

local route interface

static route

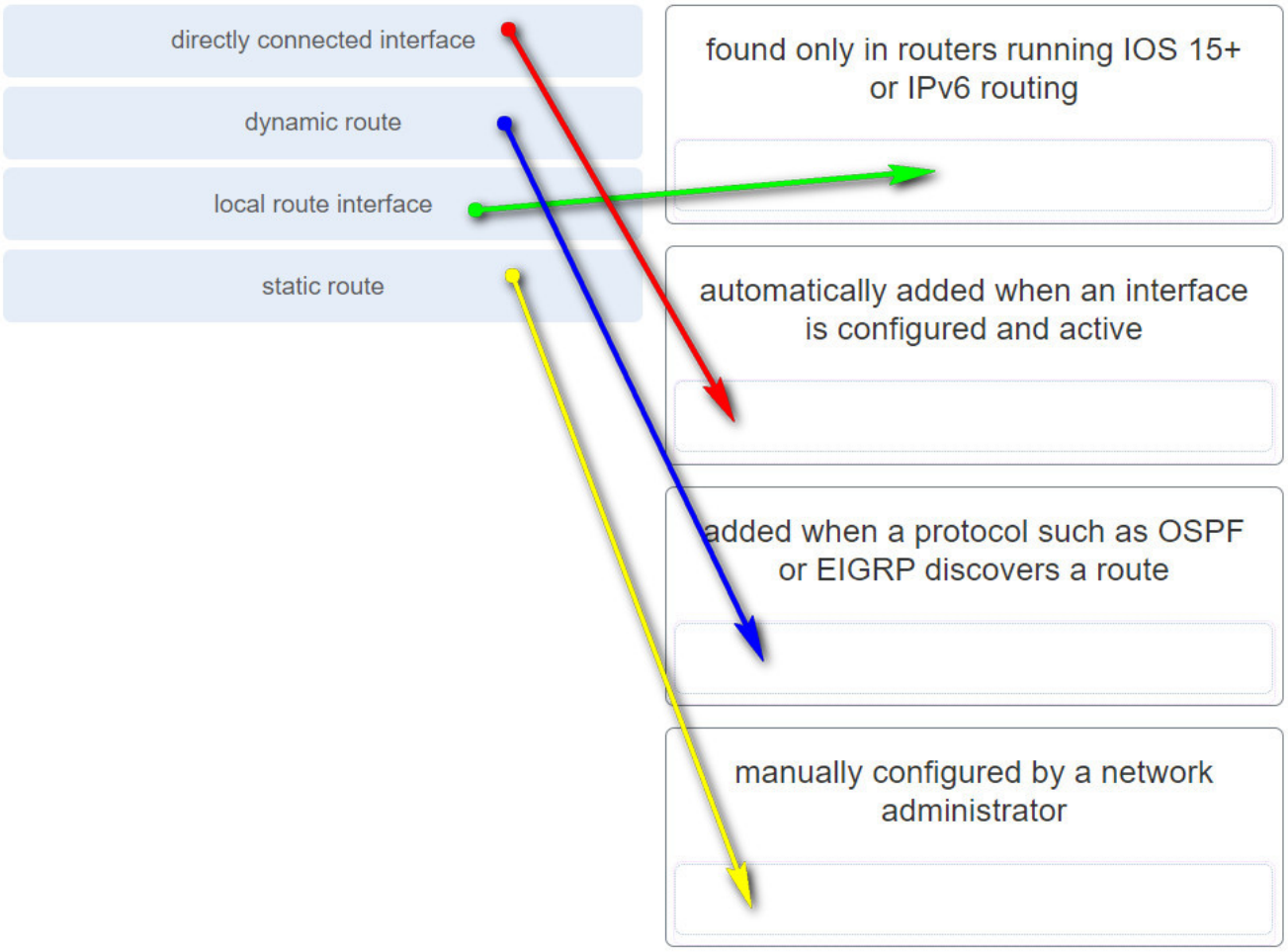
found only in routers running IOS 15+ or IPv6 routing

automatically added when an interface is configured and active

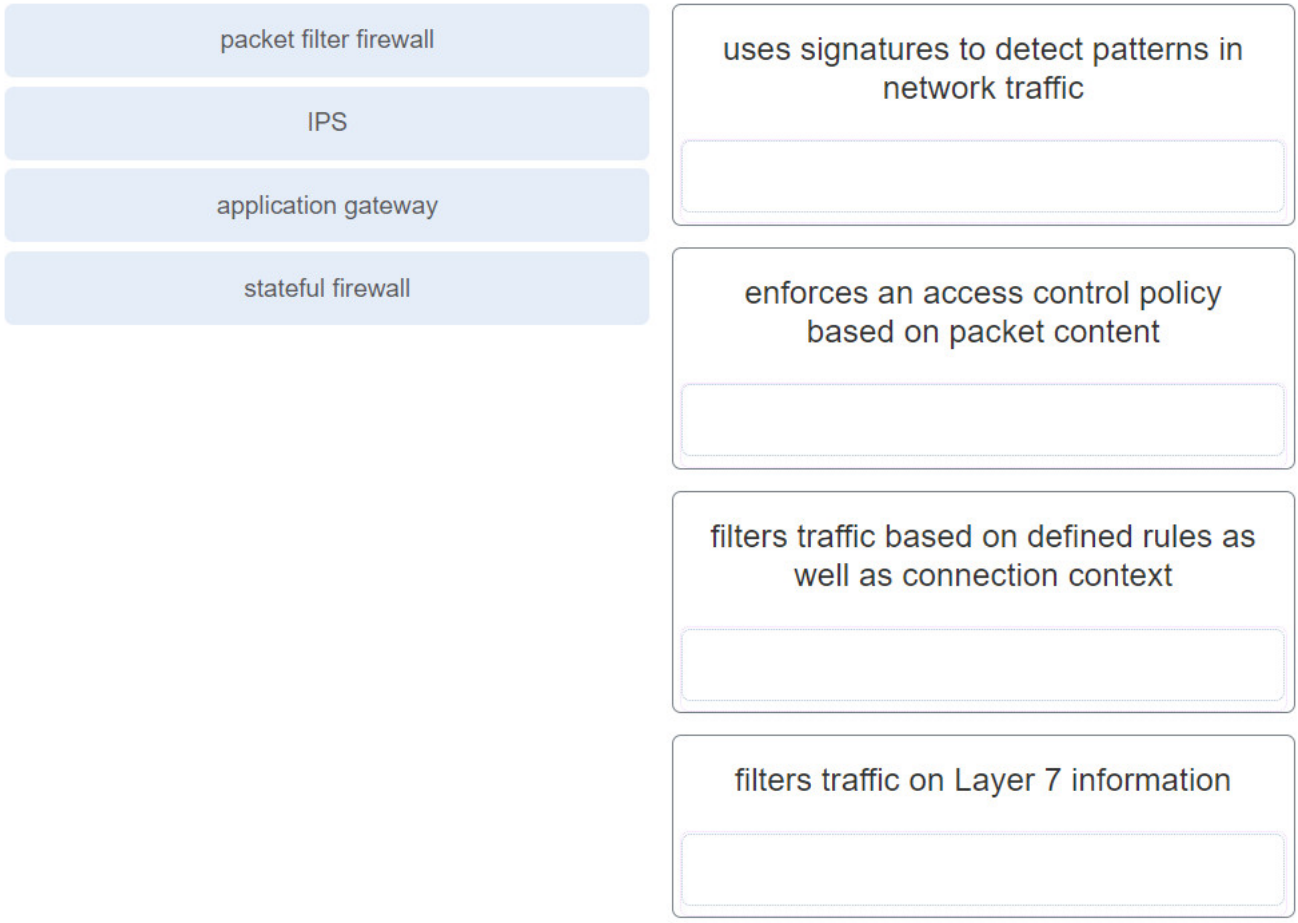
added when a protocol such as OSPF or EIGRP discovers a route

manually configured by a network administrator

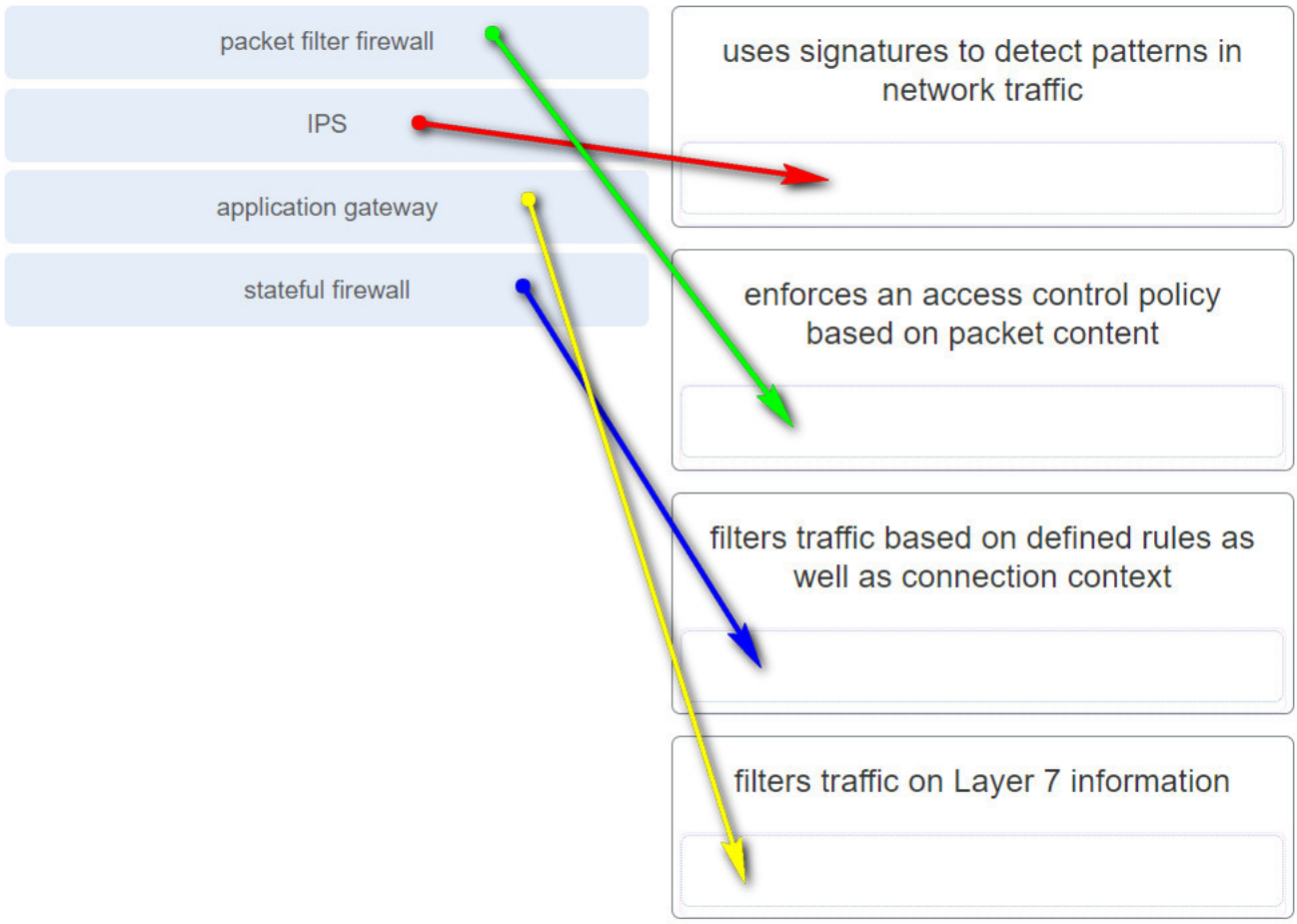
Answer



37. Match the network security device type with the description.


packet filter firewall
IPS
application gateway
stateful firewall
uses signatures to detect patterns in network traffic
enforces an access control policy based on packet content
filters traffic based on defined rules as well as connection context
filters traffic on Layer 7 information

Answer



Download PDF File below:

[sociallocker id="54558"]

CCNA Cybersecurity Operations (Version 1.1) - CyberOps Chapter 5 Exam Answers.pdf 409.63 KB 1163 downloads

...

Download

[/sociallocker]