**DV162\_4\_PAS on video related to Firewalls**

**Possible Answers Sheet**

Q1.\_\_\_\_\_\_\_\_\_\_\_\_\_\_ can be either software or hardware. It is a system that is designed to prevent unauthorized access from entering a private network by filtering the information that comes in from the internet.

A1. Firewall

Q2. Firewall blocks unwanted traffic and permits wanted traffic. So basically it filters the incoming networking data packets and determines by its access roles if it is allowed to enter the network. (True/False)

A2. True.

Q3. A firewall controls the flow of traffic coming into and out of the network through its\_\_\_\_\_\_\_\_\_\_\_ that stands for \_\_\_\_\_\_\_\_\_. It is a list of roles on what can access the network. It either allows or denies permissions.

A3. ACL, Access Control List.

Q4. IP addresses try to get into this network, firewalls would deny or allow it because of the rules that are set in the \_\_\_\_\_\_\_\_\_\_\_\_.

A4. ACL.

Q5. Most firewalls come with a default role of \_\_\_\_\_\_\_\_\_\_\_\_\_\_and what that basically means is that the firewall only allows traffic to enter to the network that the ACL specifically says that it will allow.

A5. Implicit Deny.

Q6. If your ACL only has one role and lets say that role has allowed port no. 80 which is webpages so what would that mean?

A6. That means it only allows access to web pages on the network but nothing else.

Q7. Port 25 and port 110 are given access to the network and now those ports along with their respective services are able to go through the firewall but everything else is implicitly denied. (True/false)

A7. True.

Q8. \_\_\_\_\_\_\_\_\_\_\_\_\_ is a software firewall. This is a kind of firewall that is installed on a computer only and it protects that computer only and nothing else.

A8. Host Based Firewall.

Q9. You can turn a firewall on or off if you want and you can also create an exception to a firewall based on the application name on the \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_tab.

A9. Exceptions Tab.

Q10. \_\_\_\_\_\_\_\_\_\_\_ based firewall is a combination of hardware and software. And it operates in a network layer.

A10. Network.

Q11. Network-based firewall is placed between a\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_. And unlike a host based firewall we will only protects own computer and network based firewall protects an entire \_\_\_\_\_\_\_\_.

A11. Private Network, Internet.

Q12. Network-based firewall management roles is applied to the entire network so that any harmful activity can be stopped before it reaches the computers. (True/False)

A12. True.

Q13. A \_\_\_\_\_\_\_\_\_\_\_\_\_\_firewall monitors all the connections and data streams that are passing through and a record of it.

A13. Stateful

Q14. Stateful firewall uses the connection information that comes from the \_\_\_\_\_\_\_\_\_, \_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_that in allowing or denied the flow of data packets it does a thorough job of protecting a network dynamically.

A14. Applications, previous session, factors

Q15. A \_\_\_\_\_\_\_\_\_\_\_firewall on the other hand does not do a thorough job as a stateful firewall does.

A15. Stateless.

Q16. A stateless firewall uses an ACL to allow or deny traffic. It does not thoroughly inspect the data packet. It only looks in to the header portion of the data packets. And it does not keep record of previous data packets. (True/False)

A16. True.

Q17. Content filtering is a technology that is commonly used in \_\_\_\_\_\_\_\_\_\_.

A17. Emails.

Q18. Content filtering filters data based on their content and not their source. This type of filter is commonly used to\_\_\_\_\_\_\_\_\_\_\_\_.

A18. Filter Email Spams.

Q19. \_\_\_\_\_\_\_\_\_\_\_\_ is used to detect viruses that have a well known behaviour pattern.

A19. Signature Identification.

Q20. Certain viruses and malware have a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_and that use a signature identification are programmed to spot these behaviour. And once it spotted takes action to \_\_\_\_\_\_\_\_\_\_\_ the intrusion.

A20. Common Behaviour, Block.

Q21. The intrusion detection or prevention system is a hardware tool that is typically placed between \_\_\_\_\_\_\_\_\_\_\_\_\_ and \_\_\_\_\_\_\_\_\_\_

A21. Internet, Firewall.

Q22. Intrusion detection system's job is to alert and prevent a network from outside attacks. These attacks include viruses, malware, and hackers who are trying to sabotage the internal network. (True/False)

A22. True.

Q23. Intrusion detection system monitors traffic flowing through a network looking for \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

A23. Suspicious Pattern.

Q24. If an intrusion detection system finds any it alerts the \_\_\_\_\_\_\_\_\_\_\_\_\_of a pending danger.

A24. Network Administrator.