"Firewalls"
"Q & A"

Q1. Describe the manner in which an organization develops a firewall policy that defines how their firewalls should handle inbound and outbound network traffic for specific IP addresses and address ranges, protocols, applications, and content types based on the organization's information security policies.

ANS. Q1. An organization should conduct risk analyses in order to develop a list of the types of traffic used by the organization and how this traffic must be secured, which includes the circumstances under which the traffic can traverse a firewall. Examples of policy requirements include ***permitting only*** necessary Internet Protocol (IP) protocols to pass, appropriate source and destination IP addresses to be used, particular Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports to be accessed, and certain Internet Control Message Protocol (ICMP) types and codes to be employed.

Generally, all ***inbound and outbound*** traffic not expressly permitted by the firewall policy should be blocked because such traffic is not needed by the organization. This practice reduces the risk of attack and can also decrease the volume of traffic carried on the organization's networks.

Q2. Identify all deployment requirements that should be considered when determining the locations and features of firewalls.

Ans. Q2. An organization must determine which network areas are to be protected, and which types of firewall technologies will be most effective for the types of traffic that require protection. Several important performance considerations also exist, as well as concerns regarding the integration of the firewall into existing network and security infrastructures. Firewall performance can be improved by optimizing firewall rule sets. ***For example***, some firewalls check traffic against rules in a sequential manner until a match is found; for these firewalls, rules that have the highest chance of matching traffic patterns should be placed at the top of the list wherever possible.

Choosing the type or types of firewalls to deploy and their positions within the network can significantly affect the security policies that the firewalls can enforce. Additionally, ***firewall solution design*** involves requirements relating to the physical environment and personnel as well as considerations for virtual private networks (VPNs).

Q3. Describe the important practices required in maintaining the effectiveness of a firewall.

Ans. Q3. Firewall ***performance*** must be monitored to enable potential resource issues to be identified and addressed before they become overwhelming. ***Logs and alerts*** should also be continuously monitored to identify threats—both successful and unsuccessful.

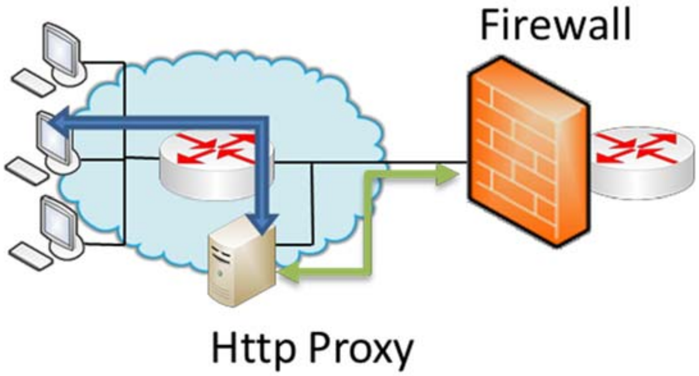
Firewall rule sets and policies should be managed by a formal change management control process with rule set reviews or tests performed periodically to ensure continued compliance with the organization's policies, because of their potential to impact security and business operations. ***Firewall*** software should be patched as vendors provide updates to address vulnerabilities.

Q4. Use a network diagram to illustrate the manner in which to use a HTTP proxy to protect outbound HTTP requests from internal hosts.

Ans. Q4. The appropriate network diagram that employs a dedicated HTTP proxy server placed behind a perimeter firewall system is shown below.

The ***HTTP proxy*** would handle outbound connections to external web servers and possibly filter active content. Requests from users first go to the proxy and the proxy then sends the request (possibly changed) to the outside web server.

The response from that web server then comes back to the proxy, which relays it to the user. Many organizations enable caching of frequently used web pages on the proxy to reduce network traffic and improve response times.



Q5. Describe the manner in which to inspect packets at a border firewall for VPNs.

Ans. Q5. A ***VPN uses additional protocols*** to encrypt and decrypt traffic and provide user authentication and integrity checking. When a decrypted packet enters an internal network, the firewall can inspect the packet in accordance with rule sets.

A firewall can also inspect the packet before encryption when leaving an internal network in accordance with rule sets. ***Placing a VPN behind a firewall*** would require VPN traffic to be passed through the firewall while encrypted, preventing the firewall from inspecting the traffic.

Q6. Describe the manner in which to use a personal firewall to protect a computer based on location and applications.

Ans. Q6. Some personal firewalls allow the creation of different profiles based on location, such as one profile for use inside the organization's network and a different one for use when at a remote location. ***This is particularly important*** when a computer is used on an un-trusted external network, ***because having a separate firewall*** profile for use on such networks can restrict network activity more tightly and provide stronger protection than would be possible when using a single profile for all networks.

Personal firewalls can also be configured to allow communications based on lists of authorized applications, e.g. web browsers using ***SSL*** (Secure Sockets Layer), which is the ***standard security technology*** for establishing an encrypted link between a web server and a browser, when contacting web servers and email clients sending and receiving email messages, while denying communications involving any other applications.

These devices are referred to as application-based firewalls. Access control is based on the applications or services launched, not on the ports or services.

Q7. Describe the limitations of firewall inspection.

Ans. Q7. Firewalls ***can only work effectively*** on traffic they can inspect. Regardless of the firewall technology chosen, a firewall that cannot understand the traffic flowing through it will not handle that traffic properly. A simple example is that of allowing traffic that should be blocked. Many network protocols use cryptography to hide the contents of the traffic; for example, ***IPsec*** and ***TLS*** (Transport Layer Security) with its predecessor being Secure Sockets Layer (SSL), Some additional encrypting protocols include ***Secure Shell*** (SSH) and ***Secure***

Real-time Transport Protocol (SRTP).

Firewalls also cannot read application data that is encrypted, such as email that is encrypted using the ***S/MIME*** (Secure/Multipurpose Internet Mail Extensions) or ***OpenPGP*** (Open Pretty Good Privacy, which defines standard formats for encrypted messages, signatures, private keys, and certificates for exchanging public keys), protocols or files that are manually encrypted.

Another limitation faced by some firewalls is understanding traffic that is tunneled, even if it is not encrypted. For example, IPv6 traffic can be tunneled in IPv4 in many different ways. The content may still be unencrypted, but if the firewall does not understand the particular tunneling mechanism used, the traffic cannot be interpreted. In all these cases, the firewall's rules will determine what to do with traffic it does not (or, in the case of encrypted traffic, cannot) understand. An organization should have policies that describe how to handle traffic in such cases, such as either permitting or blocking encrypted traffic that is not authorized.

Q8. Describe the types of traffic an organization must block using a network layer header to protect its internal routers and network performance.

Ans. Q8. An organization should block the following types of traffic at the perimeter:

- ***Traffic containing IP source routing information***, which allows a system to specify the routes that packets will employ while traveling from source to destination. This could potentially permit an attacker to construct a packet that bypasses network security controls. IP source routing is rarely used on modern networks, and valid applications are even less common on the Internet.
- ***Traffic from outside the network*** containing broadcast addresses that are directed inside the network. Any system that responds to the directed broadcast will then send its response to the system specified by the source, rather than to the source system itself. These packets can be used to create huge "storms" of network traffic for denial of service attacks. Regular broadcast addresses, as well as addresses used for multicast IP, may or may not be appropriate for blocking at an organization's firewall. Multicast and broadcast networking is seldom used in normal networking environments, but when it is used both inside and outside of the organization, it should be allowed to pass through the firewalls.
- ***Incoming traffic with a destination address*** of the firewall itself should be blocked unless the firewall is offering services for incoming traffic that require direct connections—for example, if the firewall is acting as an application proxy.
- ***Traffic with an invalid source address*** for incoming traffic or a destination address for outgoing traffic, i.e. an invalid "external" address, should be blocked at the network perimeter. This traffic is often caused by malware, spoofing, denial of service attacks, or misconfigured equipment.
- ***Outbound traffic with invalid source addresses*** should be blocked (this is often called egress filtering). Systems that have been compromised by attackers can be used to attack other systems on the Internet. The use of invalid source addresses makes these kinds of attacks more difficult to stop. Blocking this type of traffic at an organization's firewall helps reduce the effectiveness of these attacks.

(Black prints being correct)

Q.9. Firewalls block traffic between the internal network and the

(a) Internet

(b) DMZ (Demilitarized Zone; a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.)

(c) All of the above

Q.10. VPN (Virtual Private Network is a method *used to add security and privacy* to *private* and *public* networks, like WiFi Hotspots and the Internet. VPNs are most often used by corporations to protect sensitive data) traffic is allowed through the firewall.

(a) True

(b) False

Q.11. A firewall passes or blocks traffic based upon

(a) IP address

(b) Port number

(c) All of the above

(d) None of the above

Q.12. A firewall is typically located at only one position in an organization.

(a) True

(b) False

Q.13. Packet filtering firewalls provide

(a) Stateless inspection (A stateless firewall filter, also known as an *access control list* (ACL), does not statefully inspect traffic. Instead, it evaluates packet contents statically and does not keep track of the state of network connections)

(b) Stateful inspection (known as *dynamic packet filtering*, is a firewall technology that monitors the state of active connections and uses this information to determine which network packets to allow through the firewall.)

(c) All of the above

(d) None of the above

Q.14. A proxy gateway (a gateway server that separates the network from *external networks* {*typically the Internet*} and a firewall that protects the network from outside intrusion and *allows data to be scanned* for security purposes before delivery to a client on the) operates at only the application level.

(a) True

(b) False (Circuit {session level-Transmission Control Protocol (TCP) or User Datagram Protocol (UDP)} level gateways & application level gateways do exist)

Q.15. Stateless packet filtering is performed on a per-packet basis.

(a) True

(b) False

Q.16. In stateless packet filtering, the context of the packet is examined.

(a) True

(b) False (It only evaluates packet contents)

Q.17. In a stateful filtering environment, filters can be bypassed with VPN using IP tunneling.

(a) True
(b) False

Q.18. SOCKS are a __.

(a) Application-level gateway
(b) Circuit–level gateway
(c) Internet protocol
(d) None of the above

Q.19. SOCKS perform at the ___ layer of the OSI model and below.

(a) Application
(b) Presentation
(c) Session
(d) Transport
(e) Network

Q.20. It is easy to track the state of ___ in a stateful packet filter.

(a) TCP
(b) UDP
(c) ICMP
(d) All of the above

Q.21. An effective tool used by an attacker to move their toolkit onto the system is

(a) TFTP (Trivial File Transfer Protocol is an Internet software utility for transferring files that is simpler to use than the File Transfer Protocol (FTP) but less capable. It is used where user authentication and directory visibility are not required)
(b) FTP
(c) ICMP
(d) All of the above

Q.22. An attacker can be prevented from learning a network by blocking ICMP host unreachable at the firewall.

(a) True
(b) False

Q.23. A typical firewall has the following interfaces:

(a) Outside
(b) Inside
(c) DMZ
(d) All of the above