Firewall

1. ACLs on routers slow throughput of a heavily used system resource. List two advantages of using ACLs. List a situation in which you might want to block (reject) certain traffic through an ACL on a router; that is, a situation in which the performance penalty would not be the deciding factor.
2. What information might a stateful inspection firewall want to examine from multiple packets?
3. Recall that packet reordering and reassembly occur at the transport level of the TCP/IP protocol suite. A firewall will operate at a lower layer, either the Internet or data layer. How can a stateful inspection firewall determine anything about a traffic stream when the stream may be out of order or damaged?
4. Do firewall rules have to be symmetric? That is, does a firewall have to block a particular traffic type both inbound (to the protected site) and outbound (from the site)? Why or why not?
5. The FTP protocol is relatively easy to proxy; the firewall decides, for example, whether an outsider should be able to access a particular directory in the file system and issues a corresponding command to the inside file manager or responds negatively to the outsider. Other protocols are not feasible to proxy. List three protocols that it would be prohibitively difficult or impossible to proxy. Explain your answer.
6. How would the content of the audit log differ for a screening router versus an application proxy firewall?
7. Cite a reason why an organization might want two or more firewalls on a single network.
8. Firewalls are targets for penetrators. Why are there few compromises of firewalls?
9. Should a network administrator put a firewall in front of a honeypot (introduced in Chapter 5)? Why or why not?
10. Can a firewall block attacks that use server scripts, such as the attack in which the user could change a price on an item offered by an e-commerce site? Why or why not?
11. Why does a stealth mode IDS need a separate network to communicate alarms and to accept management commands?
12. One form of IDS starts operation by generating an alert for every action. Over time, the administrator adjusts the setting of the IDS so that common, benign activities do not generate alarms. What are the advantages and disadvantages of this design for an IDS?
13. Can encrypted email provide verification to a sender that a recipient has read an email message? Why or why not?
14. Can message confidentiality and message integrity protection be applied to the same message? Why or why not?
15. What are the advantages and disadvantages of an email program (such as Eudora or Outlook) that automatically applies and removes protection to email messages between sender and receiver?