Due April 29, 2024 (Monday) at Midnight

The first eight problems are for all students. Each of the problem is worth 10 points.

Problems 16.9, 16.10, 16.11, and 17.2, 17.3 from our textbook;

Problem 6 (Kaufman's book, Chapter 17, page 439, problem 7)
Referring to Figure 17-2, suppose A and B are using IPsec in transport mode, and F1 and F2 have established an encrypted tunnel using IPsec. Assume A sends a TCP packet to B. Show the relevant fields of the IP header(s) as given to A's IP layer, as transmitted by A, as transmitted by F1, and as received by B.

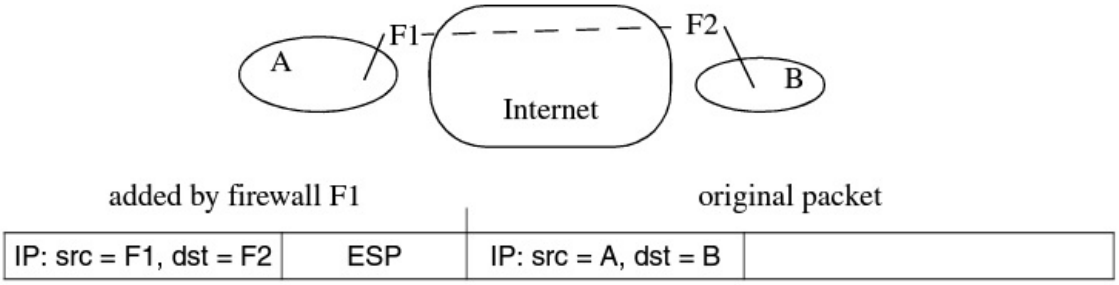

Figure 17-2. IPsec, tunnel mode, between firewalls

Problem 7: (Firewall)
The Table below shows a sample of a packet filter firewall ruleset for an imaginary network of IP address that range from 192.168.1.0 to 192.168.1.254. Describe the effect of each rule. (Hint: 192.168.1.1 is the IP address of the Firewall)

Table 22.3 Sample Packet Filter Firewall Ruleset

	Source Address	Source Port	Dest Address	Dest Port	Action
1	Any	Any	192.168.1.0	> 1023	Allow
2	192.168.1.1	Any	Any	Any	Deny
3	Any	Any	192.168.1.1	Any	Deny
4	192.168.1.0	Any	Any	Any	Allow
5	Any	Any	192.168.1.2	SMTP	Allow
6	Any	Any	192.168.1.3	HTTP	Allow
7	Any	Any	Any	Any	Deny

Problem 8: (IDS: Password management)
Assume that passwords are selected from four-character combinations of 26 alphabetic characters. Assume that an adversary is able to attempt passwords at a rate of one per second.

(a). Assuming no feedback to the adversary until each attempt has been completed, what is the expected time to discover the correct password?

(b). Assuming feedback to the adversary flagging an error as each incorrect character is entered, what is the expected time to discover the correct password?

For 471 students only:

Problem 9 (Kaufman's book, Chapter 17, page 439, problem 5)
In IPSec tunnel mode, when sending encrypted traffic from firewall to firewall, why does there need to be an extra IP header? Why cannot the firewall simply encrypt the packet, leaving the source and destination as the original source and destination?

For 571 students only:

Problem 10: (IDS: base-rate fallacy)
A taxicab was involved in a fatal hit-and-run accident at night. Two cab companies, the Green and the Blue, operate in the city. You are told that:

- 90% of the cabs in the city are Green and 10% are Blue.
- A witness identified the cab as Blue.

The court tested the reliability of the witness under the same circumstances that existed on the night of the accident and concluded that the witness was correct in identifying the color of the cab 90% of the time. What is the probability that the cab involved in the incident was Blue rather than Green?