1. (This exact question will be on the final. Prepare your answer before the exam) Make an architecture diagram of an ecommerce web site that attempts to keep order information (including personal and credit card information) private. The system must allow users to access the web site from the Internet while confidential data must be stored in the internal corporate network.
   1. Use components such as firewalls, VLANs, proxies, machine access control lists, and encryption.
   2. Explain the specific function of each of the components.
   3. Given the access control permission for each machine and firewall rules.
   4. Give the steps of how customer order information is collected and moved to the internal database. By “steps,” give the machines the data visits and the function of the machine.

See slides (e.g., see diagrams on slides 55-56 and descriptions on other slides)

1. Define and discuss (with one or a few sentences)
   1. Firewall
   2. The DMZ
   3. reverse proxy
   4. forward proxy
   5. VLAN
   6. NAT
2. What is a reverse proxy as compare to a forward proxy?
3. Compare a firewall to a proxy.
   1. Similar: both check connections according to access control rules
   2. Different: firewall examines packets as the go by, proxy: connections terminate at the proxy and new connection is made out of the proxy on behalf on the incoming connection
4. How does a NAT improve security? (less likely)
   1. Hiding IP address (private IP address 192.168.. 10….., 172….)
   2. Blocks inbound connections (unless a rule states otherwise, whitelist)
5. Why would two different engineering development groups have their network separated by a firewall?
   1. Need to know. Specifically, if the engineering groups do not work on the same project and do not need to share data, then they groups should be separated, perhaps into two networks with a firewall between the networks.
6. Is it necessary to carefully examine the logs of a firewall between two different engineering groups? What might one learn?
   1. Yes. Policy states that information separation, then this need to be checked. Also, any attempts at infiltrating the network by an employee is against policy and must be checked.
7. How can a VLAN provide security between work groups?
   1. See lecture
8. Compare and contrast a VLAN to machine access control lists
   1. The similar goals in that they limit access between machines. It is good to have both for “defense in depth” (layers of security)
   2. VLAN is controlled by network admin
   3. Machine access control is controlled system/machine admin. A successful attack might be able to change the machine access control.
9. What is a backdoor?
   1. A program on a machine that allows an attacker to login and access the machine
10. If a backdoor is opened on a web server, what type of component can block its use and explain how
    1. a firewall
       1. block connections to unknown server ports, which includes the port that the backdoor is listening on
    2. the DMZ
       1. no. this will not help.
    3. a proxy
       1. allows the network access control rules to be set so that the server to only accept connections from the proxy and therefore block connections from the attacker to the backdoor.
    4. a VLAN
       1. If a firewall is used, then the attacker cannot reach the backdoor from the internet. But it a machine behind the firewall is infiltrated or if the attacker is an employee, the backdoor can be reached from behind the firewall. In these cases, using VLAN to make a separate network for the server and the machine that the server needs to access, which will block access to the backdoor from other machines behind the firewall.
11. If a database is in the DMZ, what components might stop a user from directly logging in to the database (explain)
    1. A firewall
    2. The DMZ
    3. A forward proxy
    4. A reverse proxy
    5. A VLAN
    6. A NAT
    7. Other

Very similar to the backdoor

1. What is the principle of fail-safe defaults? How does access control based on white-list vs. access control based on black-list related to this principle?
   1. White-list means that only machines on the white list can access a server. As a result, by default machines are not on the list and therefore, by default, machines do not have access to the server = fail-safe default. A black list means that machines in the black list cannot access the server. By default, a machine can access the server. Black lists only provide minimal protection.