Tut 4.

1. Firewall :
   1. 3:
      * Packet filter.
      * circuit-level proxy.
      * application-level proxy.
   2. DMZ
      * Trong mạng máy tính, DMZ là một tiểu mạng physical hay logical ngăn cách mạng nội bộ cục bộ (LAN) với các mạng không tin cậy khác, thường là Internet. Đối với các máy chủ bên ngoài, tài nguyên và dịch vụ được đặt trong DMZ để họ có thể truy cập từ Internet, nhưng phần còn lại của mạng LAN nội bộ vẫn không thể truy cập. Điều này cung cấp thêm một lớp bảo mật cho mạng LAN : nó hạn chế khả năng truy cập trực tiếp máy chủ nội bộ và dữ liệu qua Internet của tin tặc.

2.

a/Các ứng dụng được lập trình để sử dụng TLS. Do đó TLS không thể được thấy được từ tầng ứng dụng nên không thể sử dụng trực tiếp cho VNP.

b/Sử dụng một NIC ảo (Network interfaces) . Các ứng dụng bình thông thường sử dụng NIC ảo này để việc truyền dữ liệu.Tuy nhiên NIC không được kết nối với internet, thay vào đó nó được kết nối với một ứng dụng VPN đặc biệt có sử dụng TLS và sử dụng một NIC thông thường kết nối với internet.

c/ Ipsec nằm dưới tần TCP trong các tầng giao tiếp,giữa tầng TCP/UDP và tầng IP. Do đó ứng dụng sử dụng giao thức UDP không bị ảnh hưởng bởi IPSec và IPSec có thể trực tiếp được sử dụng trong một VPN. Tuy nhiên, kể từ khi Ipsec mất một giao thức thiết lập key, một Ipsec được sử dụng trong VPN đòi hior một giao thực để cài đặt key cho Ipsec,ví dụ IKEv2.

3.

a/NIDS là một hệ thống bảo mật mạng tập trung vào những tấn công bên trong network (authoried user), giám sát tất cả các thiết bị trong hệ thống mạng. Nếu phát hiện ra tấn công hoặc hành vi bất thường, nó sẽ gửi cảnh báo về adminstrator.

HIDS chạy ở từng host cụ thể trong hệ thống mạng. Một HIDS giám sát các gói tin đến và đi từ một thiết bị và cảnh bảo người dùng hoặc adminstrator nếu phát hiện các hoạt động khả nghi.

c/Thuận lợi:

- Các mối đe dọa có thể được phát hiện mà không sợ database cập nhập.

- Bảo trì khi hệ thống cập nhập, nó sẽ tự học và tự động xây dựng profiles.

d/ Giám sát các gói tin trên đường truyền và so sánh nó với database of signatures hoặc các thuộc tính từ các mối đe dọa đã biết để phát hiện.