WLANs and VPNs

- A Virtual Private Network (VPN) uses authentication and/or encryption to allow users to access a private network from a public network (Internet).

- Typical VPNs use the Point-to-Point Tunneling Protocol (PPTP), which supports several authentication protocols.

- PPTP can be used to establish an encrypted connection over TCP/IP links, usually between the home and office networks.

- WLANs are increasingly being deployed onto the existing VPNs. The basic process for a Station to associate with an AP in a VPN is as follows:

  - The STA receives a private IP from the DHCP server.
  - Using the private IP, the STA then connects to a VPN server and sends it the user's authentication information (username and password).
  - The VPN server verifies the authentication information and returns a routable IP address to the STA.

- All outbound traffic from the STA is sent through a PPTP tunnel to the VPN server, which transmits the packet to its final destination.

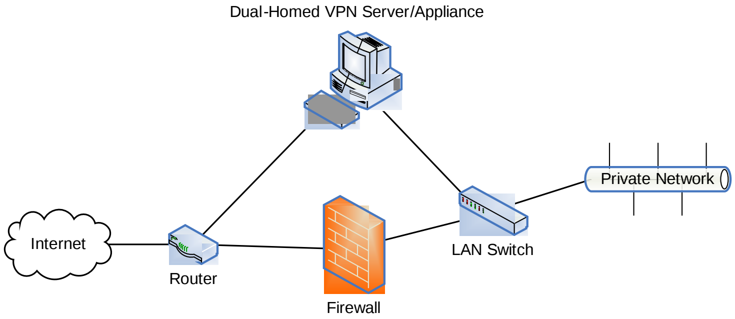
- The inbound, return traffic is received by the VPN server and then transmitted to the STA via the PPTP tunnel.

- Inserting a wireless network into an existing VPN network required careful equipment placement.

- Always keep in mind that WLAN security level and authentication should match the WIRED network

Simple Designs

- The following diagram illustrates a typical (and simple) network architecture that has a VPN server running parallel to a perimeter firewall.



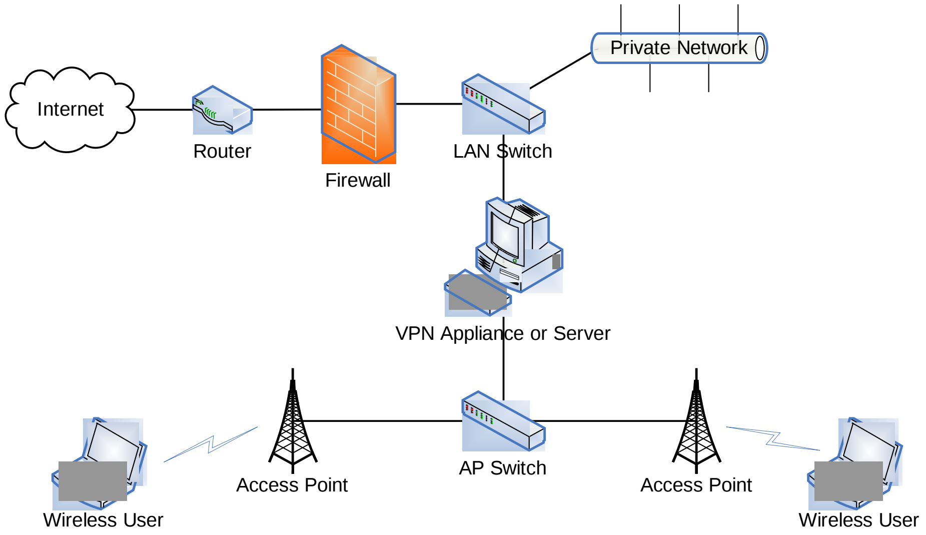
VPN server running parallel to a perimeter firewall

- The simplest option would be to insert a WLAN Access Point either on the Internet perimeter or directly into the LAN switch.

- Both these approaches have very serious drawbacks:

    - Connecting directly into the LAN switch will bypass all the firewall protections currently in place.
    - WLAN users will still be able to access the Internet without establishing a VPN connection.
    - The WLAN is not protected from the Internet in the same way that the private LAN is.
    - The VPN server is not protected by the firewall.
    - The VPN users are not restricted in their access to the private LAN by the firewall.

- A better design would be to connect the VPN server directly into the private LAN and then connect the WLAN to the VPN appliance.



VPN server is placed on the private network

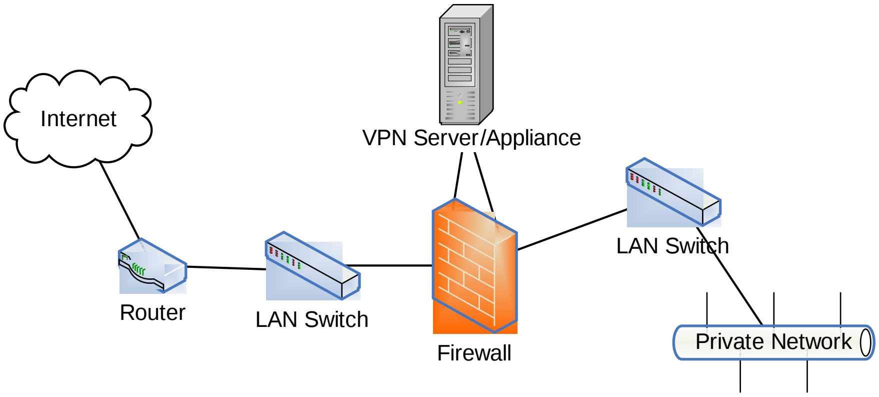
- Although this is a better design, it is very vulnerable without proper precautions taken to secure the VPN server:

    - The VPN server must be hardened and secured in order to prevent a compromise from the WLAN.
    - Ensure that policy-based filtering is implemented on the VPN. This will restrict WLAN access on the private network.

- There are some basic guidelines in implementing policies that ill restrict WLAN VPN access to resources and services:
    - Take the paranoid approach; if it is not explicitly permitted, it is denied.
    - Give careful consideration to what services WLAN users can access. For example, the they need access to the Intranet and email servers, restrict access to everything else.
    - Consider the use of thin-client solutions and browser-based applications to access services. Since this would require access to a single, fixed port on the firewall, it significantly reduces the number of entry points into the network.

<u>**Using Multihomed Perimeter Firewalls**</u>

- The following diagram illustrates a typical VPN/Multihomed firewall solution that is frequently used in traditional, wired LANs.



VPN server connected to a multi-homed firewall

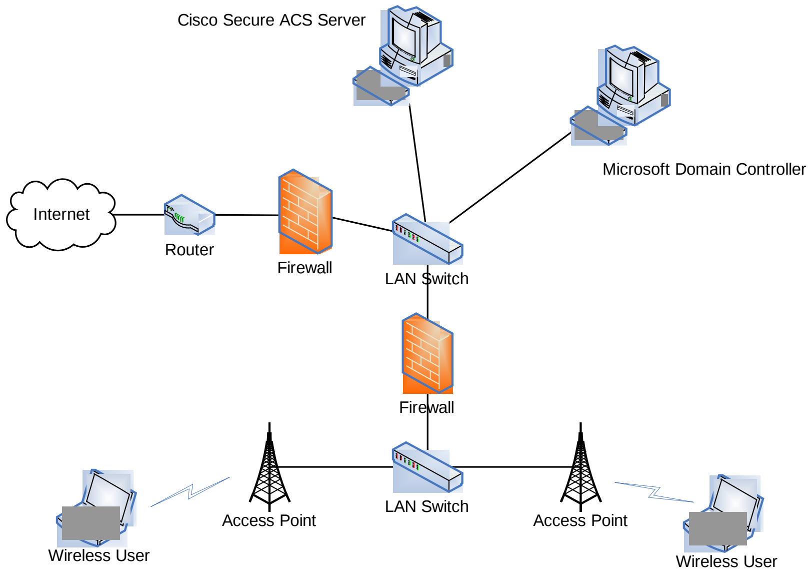
- This design provides a good security model because it limits access to the VPN server to only VPN traffic and it restricts the type and scope of access from the VPN users to the private LAN.

- The WLAN can be connected directly to the firewall, in the same way as the VPN server is.

- This type of a network architecture has the following advantages:
    - The VPN server is protected from the Internet.
    - The types of services and hosts that the WLAN users can access can be controlled and restricted.
    - The WLAN users are protected from the Internet by the perimeter firewall.

Segregated Perimeter Design

- The following network architecture is the most recommended solution because it provides the most security by physically separating the WLAN and Internet perimeters.



Two segregated perimeters for WLAN and Internet

- The WLAN perimeter must be treated as any other perimeter to an untrusted network.

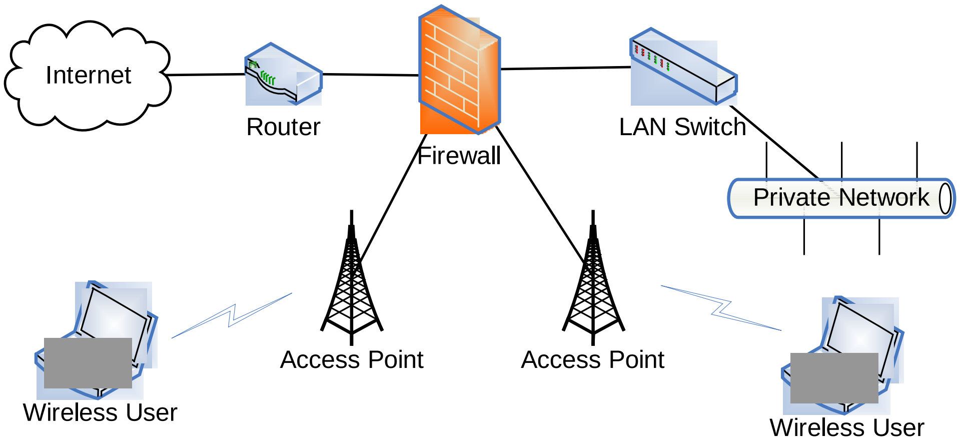
- Countermeasures must be put into place to protect the private networks from attacks that originate from the WLAN perimeter.

- The solution has the following advantages:

  - The private network is protected from the WLAN
  - The firewall can be used to restrict access from VPN users
  - WLAN users are protected from the Internet.
  - The VPN server is protected by a firewall.
  - There is no single point of failure

Small Enterprise Network

- Small or home businesses cannot invest very large amount of money into VPN hardware, so the following solution can be used for that environment.



Multi-homed firewall performing VPN and firewall services

- The above network uses a tri-homed firewall that can have some VPN capabilities built into it.

- Many low-end routers now come standard with remote user and site-to-site VPN capabilities.

- However, given the low-end hardware, many of the security functions will result in a throughput degradation through the firewall.

- Examples of such security functions are application proxies, type of encryption, etc.

- However, the architecture does provide a cost-effective solution with a reasonable degree of security.

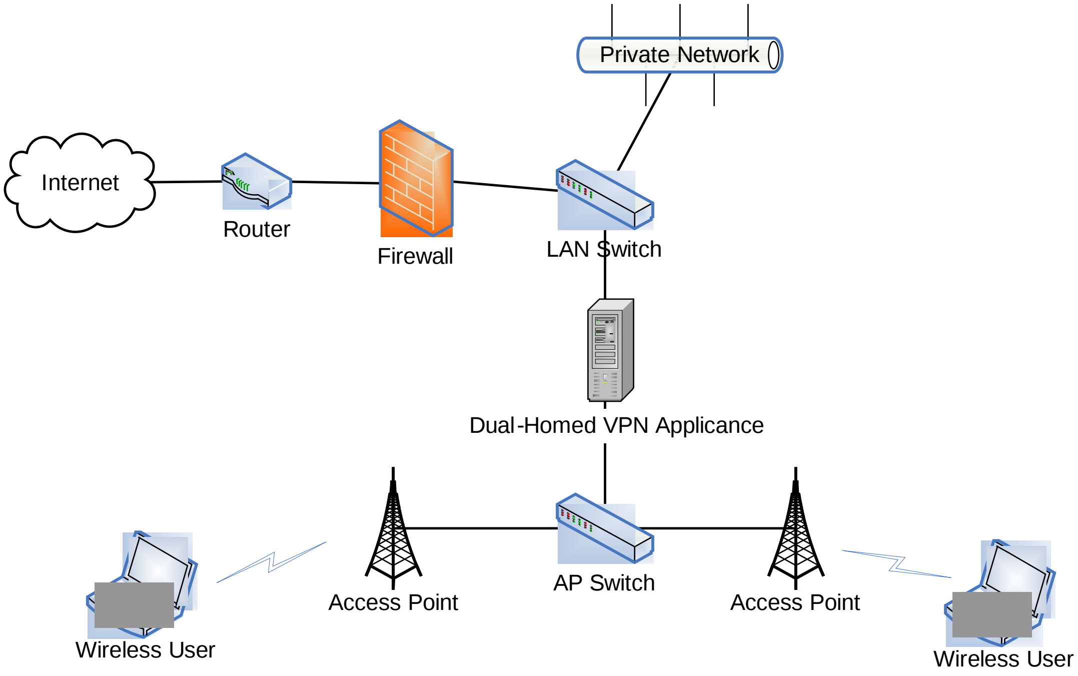
- The main design features are:

    - The multi-homed firewall with remote user VPN capabilities is used to terminate WLAN VPN connections.
    - DES encryption can be used with IPSEC (instead of PPTP), which is less CPU intensive than triple DES.
    - A shared secret key is used from the VPN client to the firewall.
    - Users have full access to the Internet, Intranet, and email.

Medium-to-Large Enterprise Network

- Larger corporate networks will require a much more sophisticated network architecture in terms of security and efficiency.

- The following diagram illustrates a large enterprise WLAN architecture, with a restricted private network.



Large enterprise WLAN with restricted private network access

- In the above network, a VPN appliance is used to perform remote access IPSEC services.

- This solution will work well within a network that already has an existing VPN appliance or a large budget to purchase additional VPN hardware.

- The main advantage here is that the VPN is separate from the firewall. This will provide a substantially better throughput performance since the VPN will not be sharing CPU cycles with the firewall.

- In addition there is no single point of failure within the network. The solution will provide a high degree of security together with interoperability.

- The main design features are:
    - IPSEC is used with triple DES. The VPN device has its own encryption processor to maintain performance.
    - RSA SecureID key fobs are used for authentication. Most VPN client software is capable of integrating challenge-only tokens (such as SecureID) seamlessly.
    - The SecureID server will need to handle up to 1000 authentications per hour during business hours, so a high-performance multi-processor server will be used.
    - The VPN appliance is placed on a physically separate perimeter with a firewall protecting the private LAN from it.
    - The private side of the VPN is connected to the firewall, thus making it easy to restrict access to WLAN users.

Securing Wireless Public Access

- Using free 802.11 as a tool to attract customers or to provide hassle-free access to network services is becoming very popular at cafes, hotels and campuses.

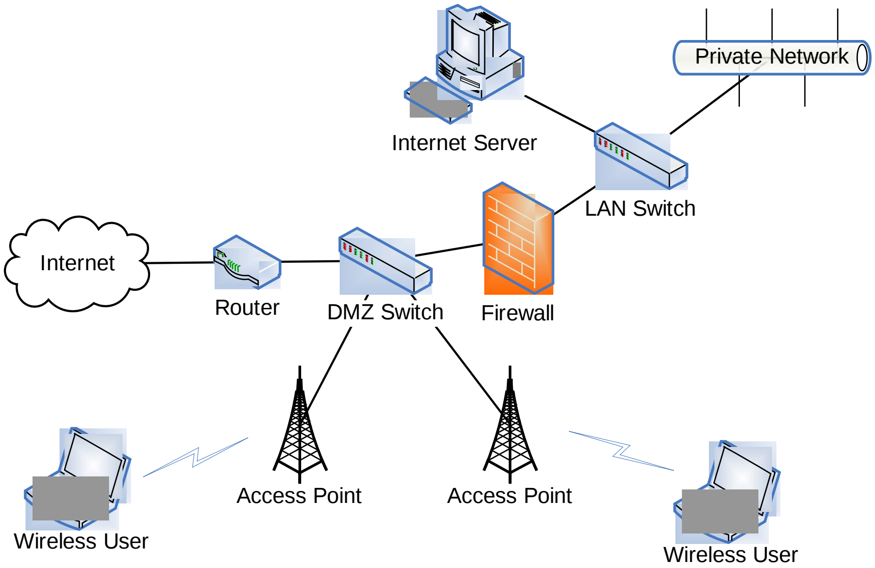
- The primary design considerations for deploying open-access networks can be summarized as follows:

  - Segregating the wireless from the wired side for Internet-only access.
  - Providing wireless Extranet (extending the Intranet to external users) access.
  - Careful consideration of new and existing firewall rules.
  - Using a VPN to allow integration of internal and guest users on the same equipment.
  - The use of encryption is avoided since this would require setup operations on the client side before the station can access the WLAN.
  - An open-access network by its very nature must avoid inconveniencing users and placing additional setup burdens on them.
  - However, users must be made aware of the risks, limitations, and restrictions of such networks.

- The most critical decision in an open-access WLAN is how to segregate the guest users from the internal, private network.

- One obvious solution is to physically separate the two networks, but this is not always practical in environments that offer services such as customer Extranet, or share Internet connections.

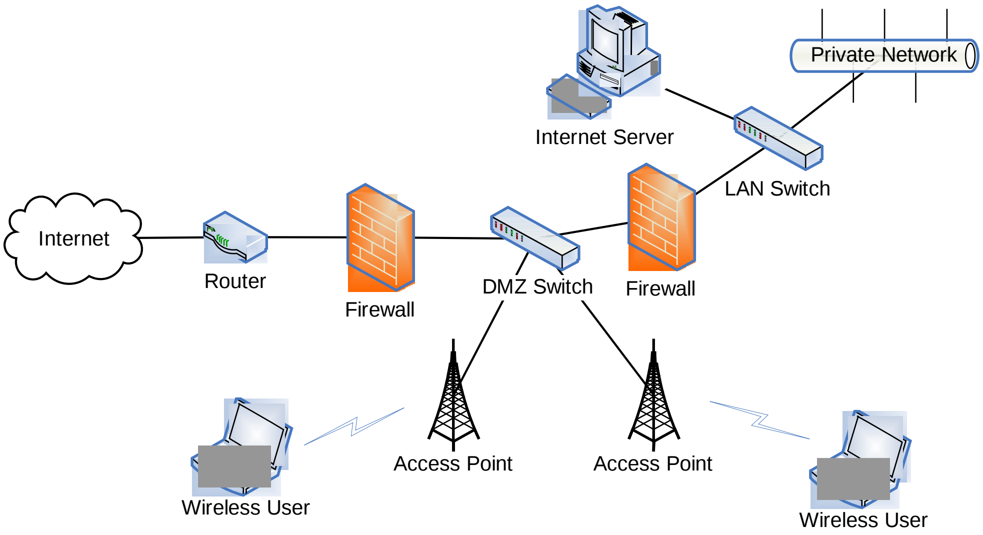
- The following diagram illustrates a simple architecture that places the WLAN components in the DMZ.



Using a firewall to segregate WLAN from the private network

- The WLAN components are not protected from the Internet, nor are they restricted in the type of access the wireless users have to the Internet.

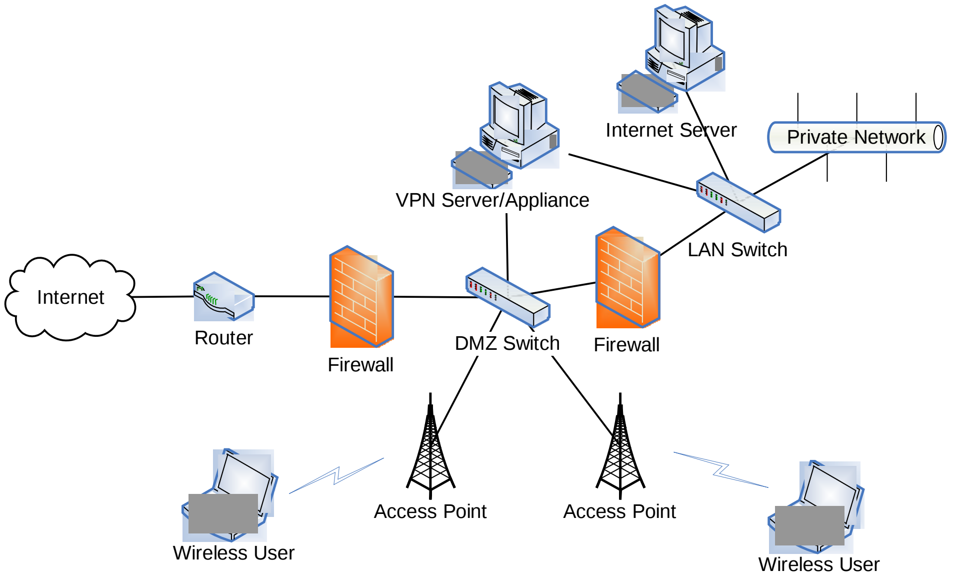
- A better solution would be to place the WLAN between a firewall for the Internet and the firewall for the private network. This is shown below.



Using two firewalls to restrict access to/from the WLAN and to/from the private network independently

- The above solution has the advantage of protecting the WLAN users from the Internet. Equally as important, it prevents WLAN users from using the network to launch attacks on other systems on the Internet.

- Yet another solution would be to use a VPN appliance that allows limited access to Internet for WLAN users, but requires an IPSEC VPN connection before allowing access to the private network.



Using a VPN appliance that allows limited Internet access for WLAN users but requires an IPSEC VPN connection before allowing entrance to the private network

Guidelines and Policies for Implementing Public Access WLANs

- Any company that offers free public WLAN access must have security at the top of its concerns.

- However, the company must also keep in mind that making it too inconvenient for users to access and use the WLAN will drive business away.

- In addition the company must also provide full internal access for authorized employees with wireless capability.

- The following general guidelines are a good starting point:

    - Provide wireless access is such a way that does not require any special configuration on the part of the guest user.
    - Limit guest user access to standard types of low-risk, low-bandwidth resources.
    - Protect guest users from attacks originating from the Internet.
    - Segregate the wireless network from the private network.
    - Provide wireless access to the internal network to authorized employees only.
    - It is a good idea to implement URL filtering to prevent objectionable or illegal material from being downloaded or uploaded.

- The following are some risks that will have to be managed and mitigated:

    - Attacks from the Internet on wireless guest users
    - Attacks from guest users to systems on the Internet
    - Attacks from guest users to the internal network
    - Lawsuits, sexual harassment complaints, hostile Environment complaints, etc., from guest users who view others viewing objectionable material.