Experiment No. 2

Isolating WLAN Traffic using Separate Firewall for VPN Connection

Background Theory

Enterprise and businesses of all sizes are concerned with corporate data being exposed due to lapses in wireless device security. With expansions to a mobile user base, companies must recognize wireless security as a valid concern. Early WLANs frequently re-used remote access VPN clients to overcome the limitations of WEP and related security concerns. But, given improvements in Wi-Fi security, does VPN still a secure communication in enterprise wireless? What are the practical benefits and limitations of using VPN over wireless? Is it all the VPN client software safe to connect?

Problem

We know that big enterprise offer laptop to its employee to provide work mobility. These laptops roam around different network accessing different information on the internet. This wide access to internet puts virus, Trojans and spyware to settle on the enterprise laptops and later on when it connects to enterprise network; it can access valuable data on the server. Further, if the same laptop makes a VPN connection with remote site, it is likely to access the remote information once it is fetched on laptop. This problem is related to site-to-site VPN connection and could be fatal if proper security procedure is not followed.

Solution

Possible solution to this problem could be to have two different i.e. internal and external firewalls. There are a number of ways to use VPN. The most common scenario is when a remote user accesses a private network across the Internet using a remote access VPN connection. In another scenario, a remote office connects to the corporate network using either a persistent or an on-demand site-to-site VPN connection (also known as a router-to-router VPN connection).

In this particular experiment we have identified common enterprise network and have simulated using OPNET (fig.1). The VPN connection was setup to a remote router and a server with applications e-mail and FTP was installed. Since there was only one firewall was present, all the traffic was send through router and present firewall. This was security breech as VPN connection and Internet connection was going through only one router. This way any other application was able to access internet and could take the valuable information out of the network.

In the second scenario two different firewalls were introduced as one Internal and one External (VPN) (fig 2). Now, with this scenario, VPN connection was possible to router as it is specified and VPN tunnel was opened between two routers through VPN firewall. This completely isolates VPN operation and avoids any security threats through VPN client software. To access internet, the external gateway is used which passes through both firewalls and prevents other unwanted
applications to access VPN tunnel. All the applications are given gateway address and gateway is connected on trusted port of the firewall.

**Set-up**

![Fig. 1 Enterprise Network](image1.png)

![Fig. 2 Modified Enterprise Network for secure VPN/Wireless Access](image2.png)
Observation/measurement

**Fig. 3 Email access through both firewall and gateway**

This graph shows email was successfully accessed after redesigning the network. The initial spike in the graph explains the entire network tried accessing the server.
Fig. 4 Declined FTP request

This graph shows FTP request was declined from server end because the rule for FTP was not set up in the internal firewall. This way no other application can reach remote server unless and until its application and port number is specified in firewall rule database.

Conclusion

This experiment shows that by using different firewalls and gateway we can isolate VPN and normal internet traffic. This is important as software VPN client does provide robust security and breeches can capture important data and send outside the network using same port on common wireless gateway.

Future plan

Future plan for this project is to expand this network to actual number of wireless nodes and number of application used on the enterprise network. Further task configuration option in the OPNET can be modified to create different applications to create security threats and solution for the same can be provided.