

# Abstract

According to the enormous development which occurred in the field of computer networks and plenty users whom are increasing day after day, and the explosive growth of the Internet, essential it has become the medium of choice for communications between most companies, government, and military organizations. The companies are using the Internet to promote their company's image, products, and services by providing World Wide Web (WWW) access to corporate Web sites. In addition to that companies can now securely and cost-effectively extend the reach of their applications and sense data across the world only to authorizer through the implementation of Virtual Private Networks (VPNs).

This research studies the procedures concerning the services, architectures, networking components, and security components that are used for VPN networks. Afterwards, the system was designed to any Company which has many branches distributed all over a wide area. The design is done by using Internet Protocol Security (IPSec) that creates a virtual tunnel to an existing Internet connection by encapsulating and encryption a real address and data which gives high security. Since the Internet is assumed to connect these companies with their branch, remote user, and partners/suppliers, the firewall must used to protect company's network from the hacker. The system implemented on a prototype of Virtual Private Network that contains five computers, one of these computers represents Internet (hacker computer), two computers for VPN Gateway that used Linux OS to provide all the functionality necessary for VPN, and the other two computers used as workstation for the Electronics Company and their branch. Finally, the analysis is performed using the results obtained from tests carried on the prototype system and get that IPSec is absolutely the more preferable choice of tunneling protocol over OpenVPN.

# الخلاصة

نظراً للتطور الكبير الذي حصل في مجال شبكات الحاسوب وكثرة عدد المستخدمين الذين يزدادون يوماً بعد يوم والنمو الحاصل في استخدام الانترنت وخاصة انه اصبح يُختار كوسط ناقل للاتصالات بين الشركات, الحكومات, والتنظيمات العسكرية. تستخدم الشركات الانترنت لإنشاء عنوان لها والترويج عن منتجاتها والخدمات التي تقدمها, وبواسطة الشبكة العنكبوتية العالمية يمكن الوصول الى موقع شبكة الشركة, بالإضافة الى ذلك تستطيع الشركات الآن بصورة آمنة وغير مكلفة ان توسع الوصول الى تطبيقاتها ومعلوماتها الحساسة عبر العالم للمخولين فقط عن طريق انجاز الشبكة الخاصة الافتراضية.

تناول البحث الاجراءات المتعلقة في التركيب والخدمات لشبكات VPN والبروتوكولات المستخدمة والمكونات الامنية التي استخدمت في التصميم. تم تصميم النظام لشركة افتراضية اسمها شركة الالكترونيات التي لديها فروع موزعة على مساحة واسعة وذلك باستخدام IPsec بروتوكول الذي يكون نفق خيالي لاتصالات الانترنت بواسطة تغليف وتشفير عنوان IP والبيانات المنقولة عبر الشركات وهذا يعطي امنية عاليةز ولانة تم استخدام الانترنت لربط هذه الشركة مع فرعها والمستخدمين عن بعد وشركائها والمجهزين لذلك يجب وضع جدار لحماية الشركة من الاختراق. وتم انجاز النظام على نموذج VPN مكون من خمسة حاسبات حيث تم استخدام احد هذه الحاسبات كإنترنت (مخترق), وحاسبتان لبوابة VPN تستخدمان Linux OS لتوفير جميع وظائف VPN, والحاسبتان الباقيتان كمستخدمين احدهما في الشركة الرئيسية والاخرى في فرع الشركة. واخيراً تم انجاز تحليل باستخدام النتائج التي استخرجت من الاختبار الذي حصل على النموذج وتم التوصل الى ان بروتوكول IPsec هو افضل اختيار لشبكات VPN من بروتوكول OpenVPN .