Acknowledgements

This work was carried out in cooperative research and development project.
Our deepest gratitude is due to my supervisor, Dr. Yahyia Abdalla Mohammed for his guidance, encouragement, and kind helpful which made this work possible.
I am, also would like to thank Engineer Nazar Elshamy for his unlimited support and helps.
And, of course, thank my family for standing beside me all the time.

Abstract

IPSec is a framework of open standards for ensuring private communications over IP networks which has become the most popular network layer security control. It can provide several types of data protection: confidentiality, integrity, data origin authentication and access protection. The most common uses is a virtual private network (VPN) which is built on top of existing physical networks that can provide a secure communications mechanism for IP information transmitted between networks.

This research seeks to assist organizations in mitigating the risks associated with the transmission of sensitive information across networks by providing practical example on implementing security services based on Internet Protocol Security (IPSec) and show how IPSec can effect on file transferring time through the networks.

Implementation of IPSec had been done in a Linux Router in two deferent LANs and the testing result shown that there is an effect in transferring time of the data with a large size. The data analysis gives a leaner equation with a factor of X (the file size) equal (0.20) before IPSec implementation and it increase to (0.21) after IPSec implementation and this increase the time of files transferring through the network.

المستخلص

أمن بروتوكول الإنترنت(IPSec) هو إطار من المعايير المفتوحة لضمان الاتصالات الخاصة عبر شبكات بروتوكول الإنترنت(IP) التي أصبحت الأكثر شعبية كمتحكم لطب قة أمن الشبكة. يمكنه توفير عدة أنواع من الحماية للبيانات : السرية والتكامل وتوثيق بيانات المنشأ وحماية الوصول. الاستخدامات الاكثر شيوعا هي شبكة خاصة افتراضية (VPN) التي بنيت أعلى الشبكات ال قائمة المادية التي يمكن أن توفر آلية لتأمين اتصالات البيانات ومعلومات بروتوكول الانترنت (IP) التي تنت قل بين الشبكات.

يسعى هذا البحث لمساعدة المنظمات في مجال التخفيف من المخاطر المرتبطة بن قل المعلومات الحساسة عبر الشبكات من خلال ت قديم مثال عملي على تنفيذ الخدمات الأمنية يعتمد على أمن بروتوكول الإنترنت (IPSec)، وتبين كيف أن أمن بروتوكول الإنترنت يمكن أن يستخدم كوسيلة لحل ال قضايا الأمنية بالشبكة.

تطبيق أمن بروتوكول الانترنت (IPSec) تم عمله في جهاز التوجيه لينكس في شبكتين محليتين مختلفتين ونتيجة الاختبار أظهرت أن هنلك أثر في زمن ن قل البيانات ذات الحجم الكبير, وتحليل البيانات أعطى معادلة خطية بمعامل ل قيمة (X وهي حجم الملف) تساوي (0.20) قبل تطبيق IPSec وزاد إلى (0.21) بعد تطبيق IPSec وهذا زاد من زمن ن قل الملفات عبر الشبكة.

Table of Contents

List of Figures

List of Tables and Charts

List of Abbreviations

Term	Definition
3DES	Triple Data Encryption Standard
ADSL	Asymmetric digital subscriber line
AES	Advanced Encryption Standard
AH	Authentication Header
BGP	Border Gateway Protocol
CA	Certificate Authority
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DSL	Digital Subscriber Line
EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FTP	File Transfer Protocol
KDC	Key Distribution Center
ICV	Integrity Check Value
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security
ISAKMP	Internet Security Association Key Management Protocol
LAN	Local Area Network
MAC	Message Authentication Code
MIT	Massachusetts Institute of Technology
NAT	Network Address Translation
NTP	Network Time Protocol
OSPF	Open Shortest Path First

RIP	Routing Information Protocol
SA	Security Association
SAD	Security Association Database
SHDSL	Single-Pair High-speed Digital Subscriber Line
SPD	Security Policy Database
SPI	Security parameters index
SSH	Secure Shell
TCP	Transmission Control Protocol
TTL	Time to Live
UDP	User Datagram Protocol
VPN	Virtual Private Network
WAN	Wide Area Network