Journal of Information Security, **2011, 2, 39-49**
doi:10.4236/jis.2011.21004 Published Online January 2011 (http://www.SciRP.org/journal/jis)

Effective and Extensive Virtual Private Network

Tarek S. Sobh, Yasser Aly
Information Systems Department, Egyptian Armed Forces, Cairo, Egypt
E-mail: *tarekbox*2000*@yahoo.com*
Received November 13, 2010; *revised December* 22, 2010; *accepted January* 4, 2011

Abstract

A Virtual Private Network (VPN) allows the provisioning of private network services for an organization over a public network such as the Internet. In other words a VPN can transform the characteristics of a public which may be non-secure network into those of a private secure network through using encrypted tunnels. This work customized a standard VPN to a newly one called EEVPN (Effective Extensive VPN). It transmits a small data size in through a web based system in a reasonable time without affecting the security level. The proposed EEVPN is more effective where it takes small data transmission time with achieving high level of security. Also, the proposed EEVPN is more extensive because it is not built for a specific environment.

Keywords: Virtual Private Network, Network Security, Secure Data Transmission

1. Introduction

Connecting to the internet using Virtual Private Networks (VPNs) [1,2] achieves a great security transmission over the internet to the users.

Most computer systems today have 3 major lines of defense: access control, intrusion detection and prevention, and data encryption. In addition, Access control and intrusion detection [3,4] are not helpful against compromising of the authentication module. If a password is weak and has been compromised, access control and intrusion detection cannot prevent the loss or corruption of information that the compromised user was authorized to access, and also it is not helpful when the intruder uses the system and software bugs to compromise the integrity, confidentiality, or availability of resources [5,6].

To improve security solution, this work introduces a customized Effective and Extensive Virtual Private Networks called (EEVPN). The proposed EEVPN used to secure war game as a web based system. It is more effective because it is faster than other VPNs where it takes less transmission time. Here we achieved this result after comparing the proposed model results with the corresponding Cisco VPN and IBM VPN results over the same data transmission.

This paper is structured as follows: Section 2 explains VPN basic definitions and some related work. Section 3 introduces the proposed model idea and implemented algorithm. Section 4 explains the experimental results and finally Section 5 contains conclusion.

2. Virtual Private Networks

VPNs reduce remote access costs by using public network resources. Compared to other solutions, including private networks, a VPN is inexpensive [7].

A VPN uses data encryption and other security mechanisms to prevent unauthorized users from accessing data, and to ensure that data cannot be modified without detection as it flows through the Internet [8,9]. It then uses the tunneling process to transport the encrypted data across the Internet. Tunneling is a mechanism for encapsulating one protocol in another protocol as shown in **Figure 1**.

2.1. VPN Architectures

A VPN consists of four main components: 1) a VPN client, 2) a Network Access Server (NAS), 3) a tunnel terminating device or VPN server, 4) a VPN protocol. In a typical access VPN connection, a remote user (or VPN client) initiates a PPP connection with the ISP's NAS via the public switched telephone network (PSTN) [10,11]. An NAS is a device that terminates dial-up calls over analog (basic telephone service) or digital (ISDN) circuits [8]. The NAS is owned by the ISP, and is usually implemented in the ISP's POP. After the user has been authenticated by the appropriate authentication method, the NAS directs the packet to the tunnel that connects both the NAS and the VPN server. The VPN server may reside in the ISP's POP or at the corporate site, depend-

ing on the VPN model that is implemented.

The VPN server recovers the packet from the tunnel, unwraps it, and delivers it to the corporate network. **Figure 2** illustrates VPN architecture. There are four tunneling protocols used to establish VPNs, and three are extensions of the Point-to-Point Protocol (PPP) [5,6,10,11]: 1) Point-to-Point Tunneling Protocol (PPTP). 2) Layer 2 Forwarding (L2F). 3) Layer 2 Tunneling Protocol (L2TP). 4) IP Security (IPSec) Protocol Suite. In this Section we will discuss IPSec with some details because IPSec can work with IP4 and IP6.

IPSec provides cryptography-based protection of all data at the IP layer of the communications stack. It provides secure communications transparently, with no changes required to existing applications [12,13].

IPSec protects network traffic data in three ways [12, 13]: 1) Authentication: The process by which the identity of a host or end point is verified. 2) Integrity checking: The process of ensuring that no modifications were made to the data while in-transit across the network. 3) Encryption: The process of "hiding" information while in-transit across the network in order to ensure privacy.

2.3 Commercial VPNs

Many companies produced a lot of VPNs deals with different data sizes. On the other hand a few works that deal with small data sizes especially less than 1 MB, because it is a special purpose for specific application such as War Game which needs high security with low time transmission.

Here we will discuss two popular VPN commercial products Cisco VPN and IBM VPN. There are different VPN products from both Cisco and IBM such as Cisco's VPN 3000 Concentrator, Cisco VPN client 3.0, Cisco Easy VPN and IBM eNetwork. Cisco's VPN (Virtual Private Network) 3000 Concentrator solution utilizes advanced PKI technology that enables mobile and remote users to securely transfer sensitive information in fully encrypted format [www.Cisco.com].

With eToken, there is only one password to remember. Users can take their authentication keys and digital certificates with them wherever they go, on a key chain or in their pocket. Full two-factor authentication can easily be implemented from any computer that runs the Cisco VPN client 3.0 via Microsoft's CAPI interface when communicating with a Cisco VPN 30XX Concentrator Series [www.Cisco.com].

Cisco Easy VPN, a software enhancement for existing Cisco routers and security appliances, greatly simplifies VPN deployment for remote offices and teleworkers. Based

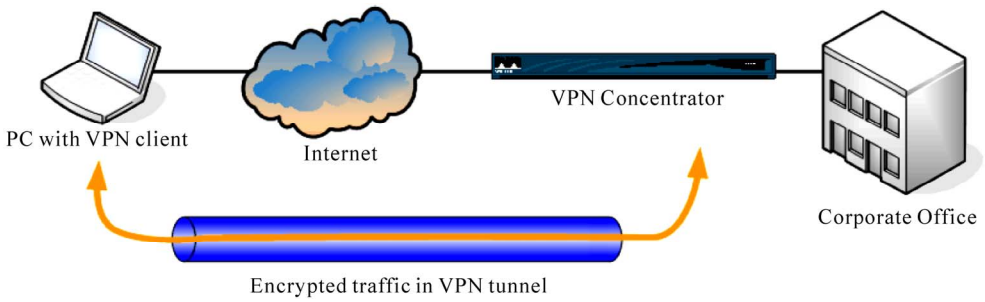

Figure 1. VPN Implementation [9].

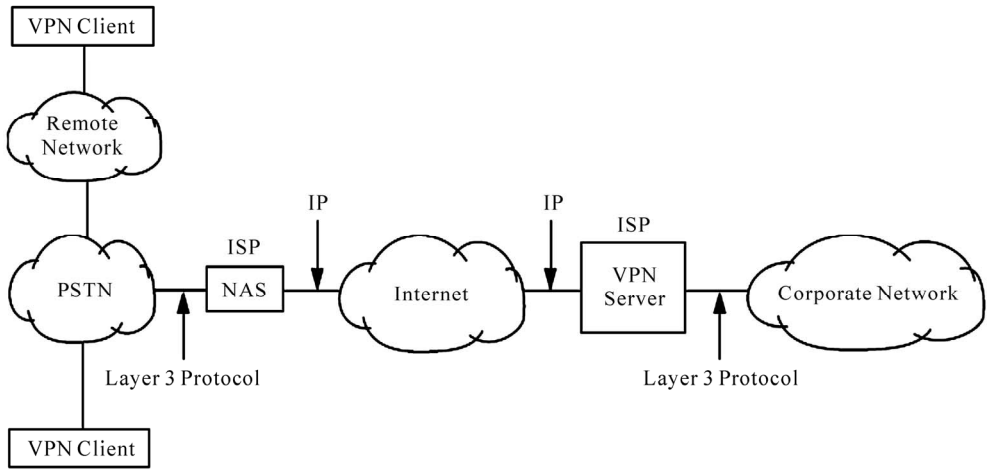

Figure 2. VPN Architecture [13].

on the Cisco Unified Client Framework, Cisco Easy VPN centralizes VPN management across all Cisco VPN devices thus reducing the complexity of VPN deployments [www.Cisco.com].

Cisco Easy VPN enables an integration of VPN remotes-Cisco routers, Cisco ASA & PIX Security Appliances, Cisco VPN concentrators or software clients-within a single deployment with a consistent policy and key management method thus simplifying remote side administration [www.Cisco.com].

eNetwork is IBM's VPN Solutions [www.IBM.com]. Here we explain briefly the implementation of eNetwork VPN and describe its value. It is based on IPSec. However, given the multitude of network environments and business needs, all scenarios have not been addressed in this section.

IBM added-value while many VPN solutions today consist only of firewalls, IBM eNetwork VPN solutions will also encompass multi-platform VPN-enabled clients and servers, routers, and management functions [www.IBM.com]. The advantages of IBM VPN solutions are: scalability; flexibility of VPN function placement; and the ability to have secure IP tunnels all the way from the client to IBM servers, where the majority of critical corporate data resides today. Also, IBM VPN solutions can be customized to be as secure or as flexible as required. It provides capabilities that can link your IT assets with Web technology to build secure e-business solutions [www.IBM.com].

2.4. War Games and VPN

War game is a simulated battle between two or more opposing fighting sides [3,4,14]. In most cases, there are two fighting sides and they are represented by the red and blue colors. Each side has its own goals to achieve at the expense of the other side, considering each side capabilities, organization, weapons, and tactical experience of management armed forces during the battle. In addition, environmental conditions such as battle terrain nature, battle timing, weather, surrounding environment must be considered. In addition to the fighting sides, one more side representing the arbitrator must be existed in the war game system. The arbitrator side is responsible of monitoring the fighting sides and evaluates their decisions.

Although it may be possible to play some forms of war games without the use of any prepared materials, most war games require a set of tools to keep track of and display data, force locations and movements, and interactions between opposing units. We have different instrumentality of war games [3,4]:

- Manual games, which represented by simple tools: maps, charts, notebook of data, and orders of battles, perhaps a set of written rules and procedures and all decisions are man-made.
- Computer-assisted games use machines ranging from desktop personal computers to very large mainframes. The machines are used to keep track of the force positions, their movement, weapon capabilities, and other critical, data-intensive pieces of information.
- Rand Corporation (fully automated) has been in the forefront of an effort to extend the role of the computer beyond that of capable assistant or sometimes opponent. This game is carried out completely on a computer, although usually with human intervention to issue orders.

The integrated software components for implementing web based war games system of each side include: 1) Operating system component 2) Database component 3) GIS component.

Securing web based war games system is very important. The main task is to achieve a high level of security to the web based war game system [5] and controlling its sides' behaviors. Since the entire network packets are going from or to the side LAN must be passed through the gateway computer, the security process is activated on the gateway computer. Encryption/decryption module is responsible of doing two tasks [14,15]. The first task is encrypting each network packet before going out from the side LAN to the web. The second is decrypting each network packet coming from the web before entering the side LAN. This is why we use a VPN for securing web based war games system. The main task of VPN here is to achieve a high level of security to the web based war games system and controlling its sides' behaviors.

3. Proposed Model

As shown in **Figure 3**, this work provides three levels of security to secure the web based war game system in the following manner:

Access control module: the access control is applied to our web based war game system using two access control mechanisms. The first mechanism is the server operating system access control mechanism. This mechanism is applied to the war game system resources (directories, files, printers …etc). The second mechanism is the DBMS access control mechanism and it is applied to the war game system database.

Virtual Private Network security module: this module is responsible of doing two tasks. The first task is encrypting each network packet before going out from the side LAN to the web. The second is decrypting each network packet coming from the web before entering the

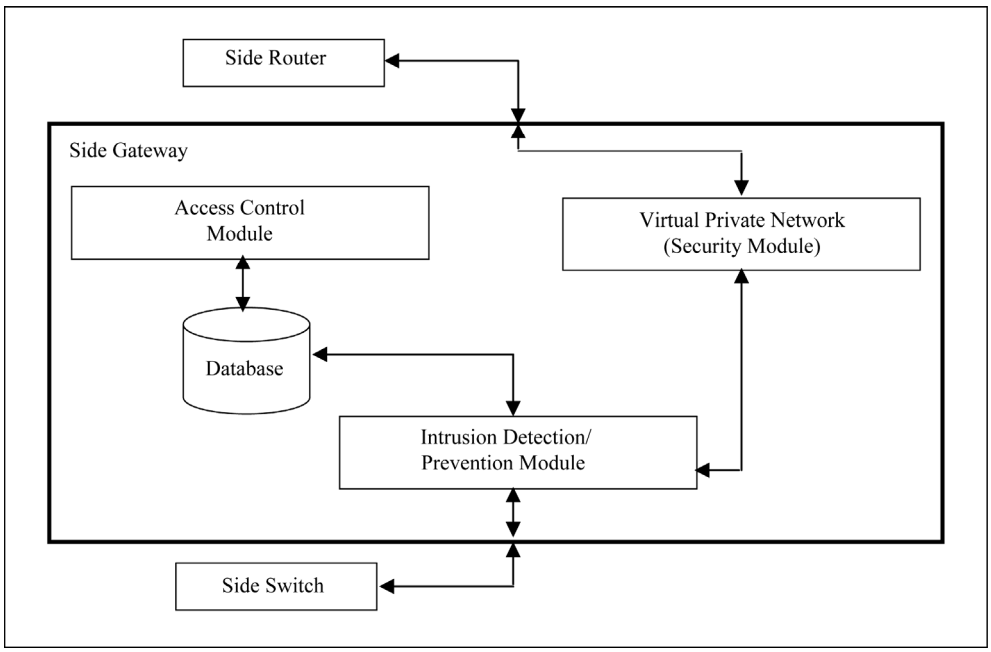

Figure 3. Security levels using a VPN.

side LAN.

Intrusion detection/prevention module: this module is responsible of checking each incoming network packet and test if it represents a normal or intrusive behavior. If the packet represents a normal behavior, the intrusion detection module forwards it to its destination; otherwise, an alarm is given to the system administrator and the packet will be blocked.

Some encryption schemes can be proven secure on the basis of the presumed hardness of a mathematical problem. Some times the secure encryption schemes it has a mathematical meaning, and there are multiple different other definitions. The proposed model use a public-key cryptography as a part from encryption schemes of VPN but it is used within our context in which the scheme will be deployed securely as shown in **Figure 3**. We customized both PPTP and IPSec for our EEVPN by erasing many overheads from them which are only needed for keeping security at large transmission time (*i.e.* large data size), so we became faster without affecting security.

EEVPN is very easy to configure and install. It is basically a wrapper for sending packets over an SSL (Ver. 3.0) connection. It supports public key encryption using client & server certificates (SSLv3). We have used a bit different approach here (*i.e.* we haven't used amvpn-keytool). **Figure 4** traces the path taken by a packet as it travels over the SSL3 tunnel created by EEVPN.

Each layer of protocol adds some bytes of overhead. This fact is illustrated in **Figure 4**. Since EEVPN just acts like a wrapper program to send packets over an SSL connection, no overhead is introduced by the EEVPN program itself. However the underlying SSL layer does add some headers. Also, we put up small ssl-timeline details about SSL handshake procedure, along with introduction to using ssldump, which is very useful to capture SSL sessions.

Figure 4 shows that the EEVPN layer produces two packets, a short packet of 29 bytes is generated with the normal packet of 152 bytes, for an input of length 128 bytes. We have found this behavior even for other wrappers like Stunnel. However, at this point, we are not yet sure as to why the shorter packet is generated and what it contains.

EEVPN does not provide mechanism to achieve compression (*i.e.* EEVPN does not support any compression mechanisms). Also no option is provided which can allow a user to select a cipher suite. The cipher suite IN USE, can be only be found out by taking the SSLdump of the session.

We conducted a series of experiments with random packet sizes and measured the packet length on the wire. The experimental results can be accessed here from the results one can conclude that EEVPN solution adds an average of 155 bytes of overhead to the data.

EEVPN uses the cryptographic functions provided by your SSL implementation plugin. Hence, if someone needs to add his own algorithm, he has to look for plug-in support in the SSL implementation that he is using or built his own code.

Currently, we are using open SSL implementation of SSL, which AFAIK does not yet support any plug-in

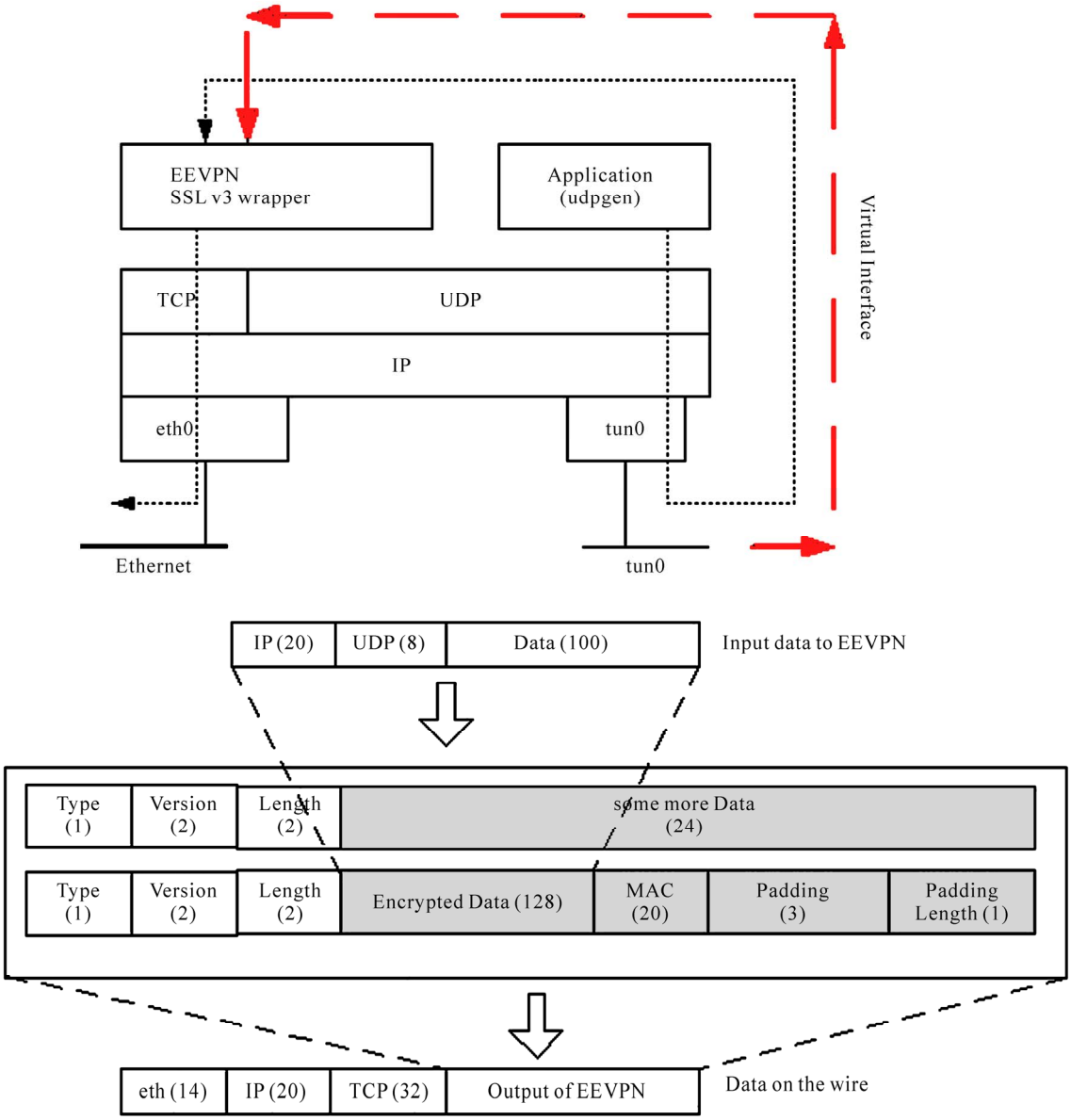

Figure 4. EEVPN layers.

algorithms to be used. However there is always the option of patching the source code itself with new algorithms and recompile the code.

The PPP-over-SSL solution for forming VPN is highly scalable. For example if a company has 'N' different sites, then it would be necessary to have O(N^2) point-topoint PPP-over-SSH links and each site will have to maintain an entry in the routing table for (N-1) other sites. It is clear a full mesh will be necessary in this case, as the complexity of maintaining any other network infrastructure will be prohibitively high.

Here the proposed EEVPN algorithm is embedded in a war game system [14] as a web based system to be one of the defense lines for securing the war game data over the public network the Internet as shown in **Figure 5**.

In our example we can now execute a war game as a web based application system in a secured manner because we will be sure from achieving authentication, integrity, and confidentiality.

[We used Microsoft visual basic 6.0 enterprise edition to design and execute the security test program]

It includes identifying the remote IP address and using encryption for data transmitted or decryption for data received.

If we send the data from side to another side without using the encryption mechanism in VPN (*i.e.* without making check for encryption), there is a possibility for hackers to get the data, modify it, or destroy it.

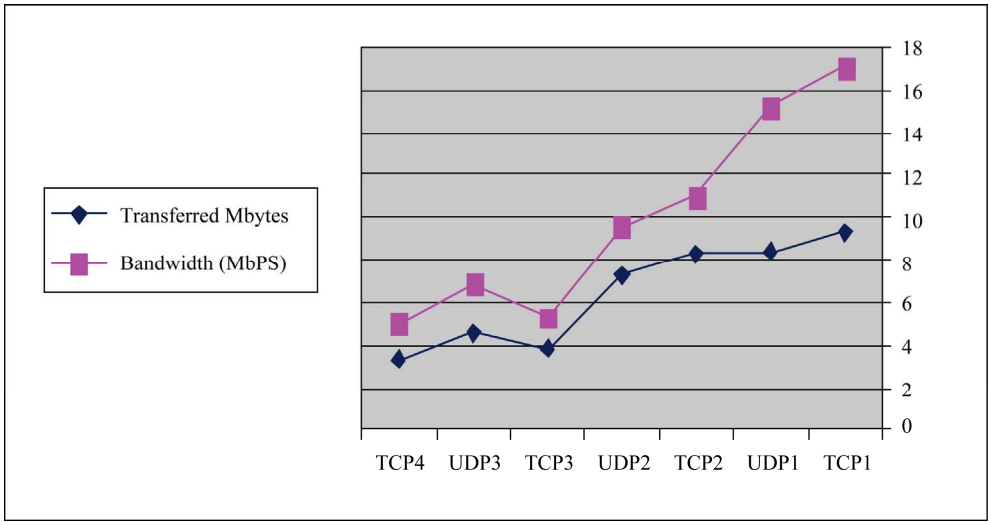

Figure 5. Hardware implementation of web based war game system.

But if we use the encryption mechanism in VPN (*i.e.* check for encryption) the data transmitted will not be understudiedable for anyone else the specific recipient how has the specific IP address, and has the decryption capability due to VPN security checks.

When the transmitted data has been received to the destination side that has the capability to decrypt the data and understand it, otherwise it will not be understandable data if not choosing VPN decryption mechanism.

Algorithm for testing security (Encryption & Decryption)

```
Sub data send
    Read (data)
    If check encryption sending is true then send encrypt (data)
        Else send (data)
End Sub
Sub load port
        Local port = value
    Remote port = value
End Sub
Sub data arrive
    If check decryption receiving is true then receive decrypt (data)
        Else receive (data)
End Sub
Sub encrypt (string)
    Loop i from 1 to length (string)
      encrypt = encrypt & key(i)
End Sub
Sub decrypt (string)
    Loop i from 1 to length (string)
      decrypt = decrypt & key(i)
End Sub
```

4. Experimental Results

Our objective is to measure & compare security level, transmission time for our created VPN with respect to other VPNs, via web based application. Measurements for transmission time with respect to data packet size:

In order to keep everything isolated, we created a new user/group (avpn/zvpn) on client (a) and server (z) using Linux command line, also passwordless login was created using SSH.

A series of tests [15-18] were run to determine the effects of a VPN connection on wireless network performance. In particular, we were interested in the performance "hit" one might take when accessing a VPN via a wireless connection (we tested a wired connection for comparison). All tests were performed using Iperf and CMPmetrics as trusted benchmarks. The First test was done using a PPTP VPN connection. The second test was done using the Cisco IPSec client for Windows 2000. The range of nodes used is between 100 and 1500 nodes.

4.1. Proposed EEVPN and Cisco VPN Results

Table 1 is a summary result of IPSec client test in case of using Cisco VPN for both plain and encrypted wireless traffic. **Table 2** is a summary result of PPTP test for plain and encrypted traffic in case of wireless connection and traditional wired traffic.

Table 3 is a summary result of proposed EEVPN with IPSec client test for both plain and encrypted wireless traffic. **Table 4** is a summary result of proposed EEVPN with PPTP test for plain and encrypted traffic in case of wireless connection and traditional wired traffic.

Figures 6-9 show another representation of the experimental output results of the above tables.

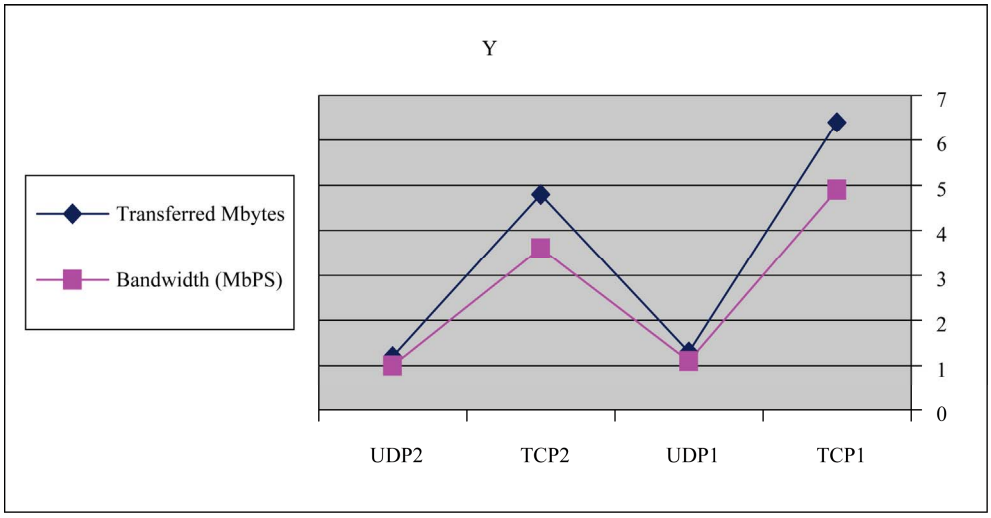

Figure 6. Cisco IPSec client test.

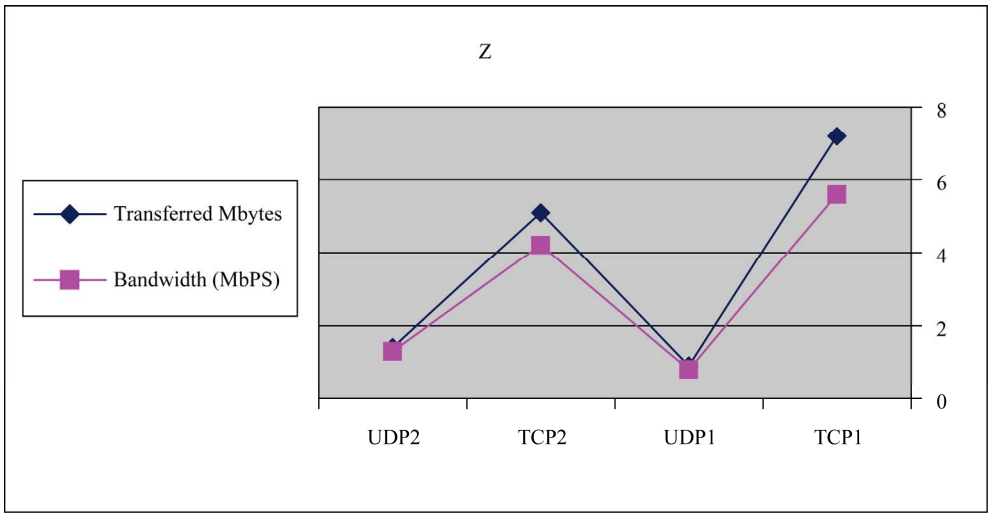

Figure 7. Proposed EEVPN with IPSec client test.

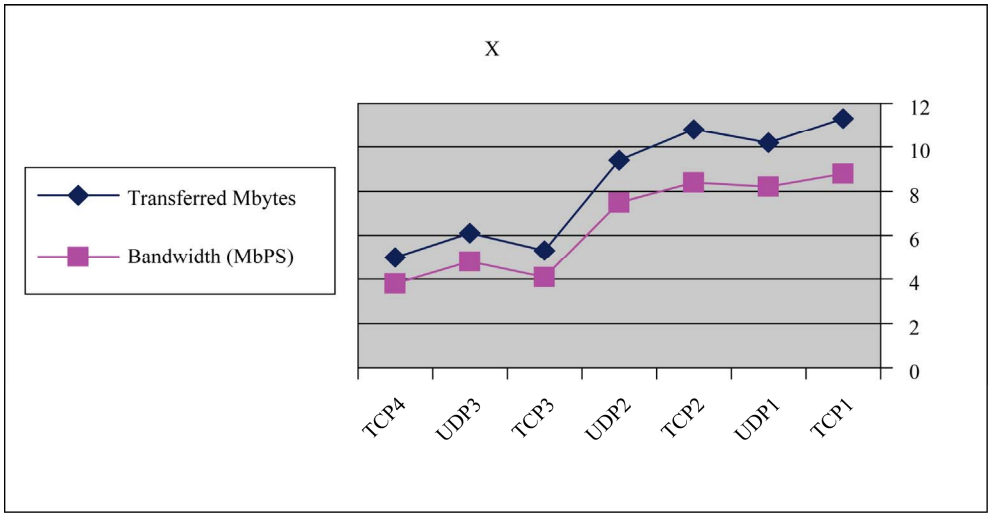

Figure 8. Cisco PPTP test.

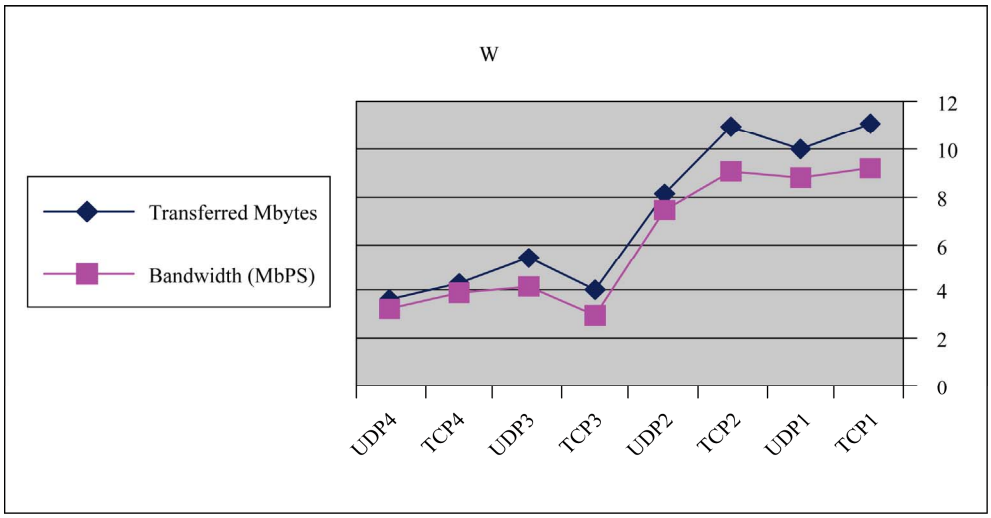

Figure 9. Proposed EEVPN PPTP test.

Table 1. IPSec client test in case of using Cisco VPN.

Test#	Protocol	Bytes (KB) transferred	Bandwidth (Mbps)
1	TCP	640	4.9
(non-encrypted wireless)	UDP	130	1.1
2	TCP	480	3.6
(encrypted wireless)	UDP	120	1.0

Table 2. Cisco PPTP test.

Test#	Protocol	Bytes (KB) transferred	Bandwidth (Mbps)
1	TCP	1130	8.8
(non-encrypted wired)	UDP	1020	8.2
2	TCP	1080	8.4
(encrypted wired)	UDP	940	7.5
3	TCP	530	4.1
(non-encrypted wireless)	UDP	610	4.8
4	TCP	500	3.8
(encrypted wireless)	UDP	470	3.8

Table 3. Proposed EEVPN with IPSec client test.

Test#	Protocol	Bytes (KB) transferred	Bandwidth (Mbps)
1	TCP	720	5.6
(non-encrypted wireless)	UDP	90	0.8
2	TCP	510	4.2
(encrypted wireless)	UDP	140	1.3

Table 4. Proposed EEVPN with PPTP test.

Test#	Protocol	Bytes (KB) transferred	Bandwidth (Mbps)
1	TCP	1110	9.2
(non-encrypted wired)	UDP	1000	8.8
2	TCP	1090	9.1
(encrypted wired)	UDP	810	7.4
3	TCP	410	3.0
(non-encrypted wireless)	UDP	540	4.2
4	TCP	430	3.9
(encrypted wireless)	UDP	360	3.2

4.2. Proposed EEVPN and IBM VPN Results

Table 5 is a summary result of IPSec client test in case of using IBM VPN for both plain and encrypted wireless traffic. **Table 6** is a summary result of PPTP test for plain and encrypted traffic in case of wireless connection and traditional wired traffic.

Figures 10-13 show another representation of the experimental output results of the above tables.

We can notice for the above figures that smaller values transferred we have better bandwidth in EEVPN than CISCO and IBM VPN, but in higher values transferred

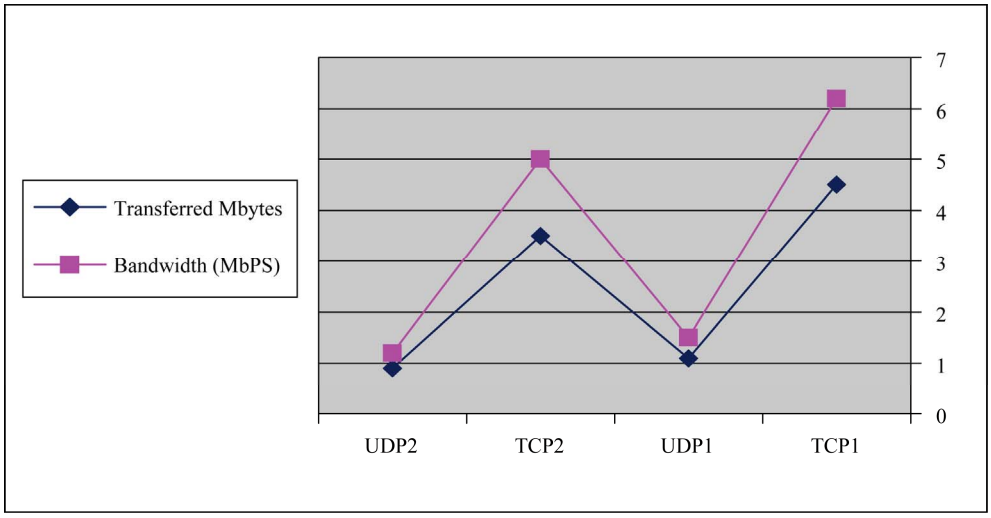

Figure 10. IBM IPSec client test.

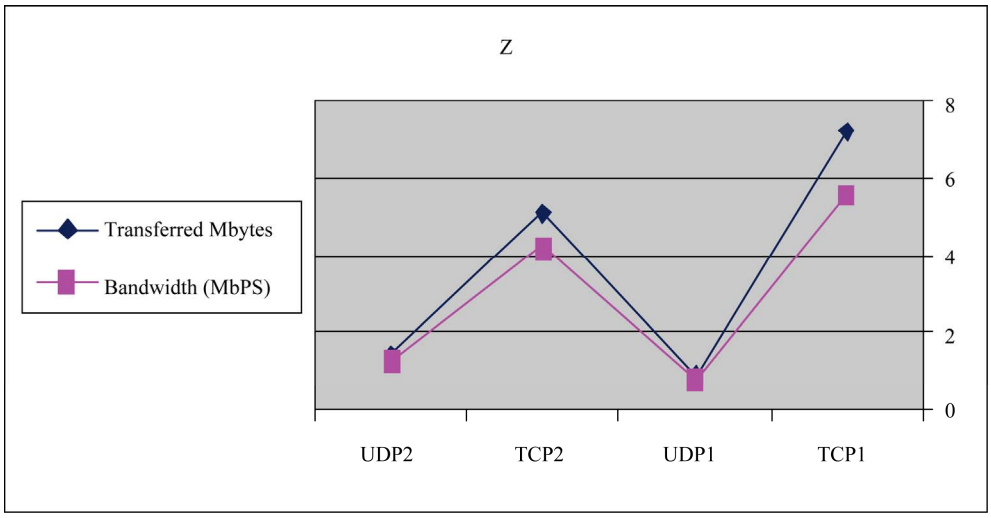

Figure 11. Proposed EEVPN with IPSec client test.

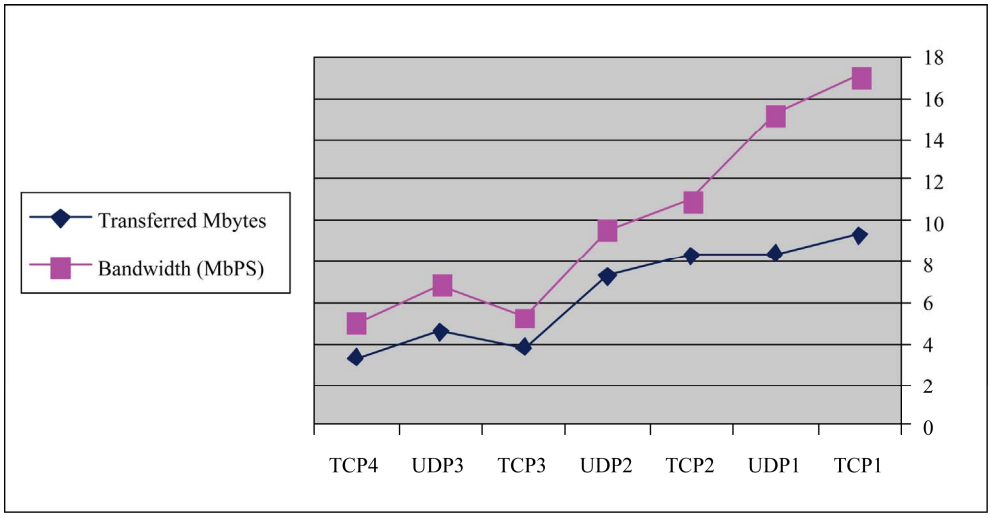

Figure 12. IBM PPTP test.

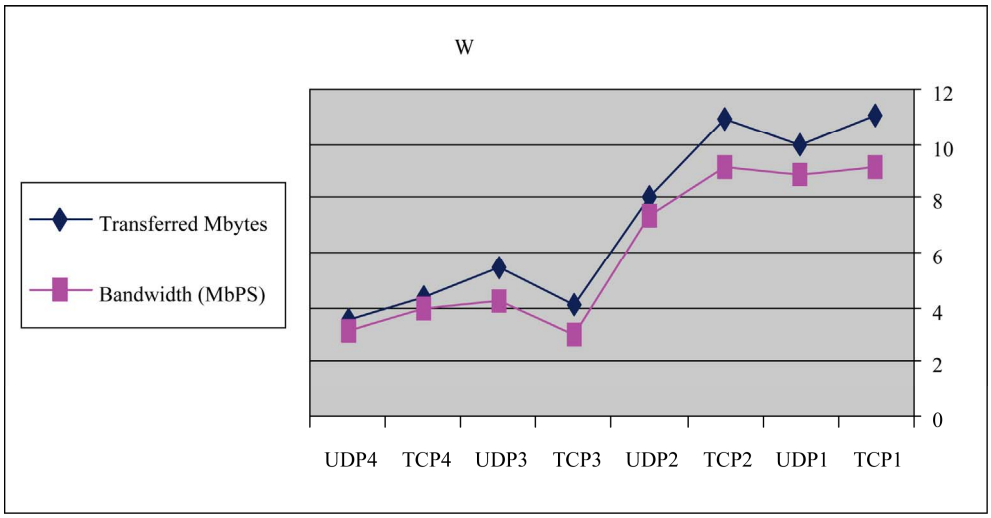

Figure 13. Proposed EEVPN PPTP test.

Table 5. IPSec client test in case of using IBM VPN.

Test#	Protocol	Bytes (KB) transferred	Bandwidth (Mbps)
1	TCP	620	4.5
(non-encrypted wireless)	UDP	150	1.1
2	TCP	500	3.5
(encrypted wireless)	UDP	120	0.9

Table 6. IBM PPTP test.

Test#	Protocol	Bytes (KB) transferred	Bandwidth (Mbps)
1	TCP	1710	9.3
(non-encrypted wired)	UDP	1520	8.4
2	TCP	1100	8.3
(encrypted wired)	UDP	960	7.3
3	TCP	530	3.8
(non-encrypted wireless)	UDP	690	4.6
4	TCP	500	3.3
(encrypted wireless)	UDP	490	3.5

we have better bandwidth in CISCO and IBM VPN than EEVPN.

Comparing results ensures that low transmission time is for EEVPN.

We can say that if we will transfer smaller values of bytes, it is better to use EEVPN, like in our implementation in which we secured a war game, we will deal with smaller values of bytes, keeping high security level which we tested using our program & trying to hack messages during data transmission to ensure data integrity & confidentiality.

5. Conclusions

This work customized a standard Virtual Private Networks (VPN) to a newly one called EEVPN (Effective Extensive VPN). In fact we need to transmit a small data size in our example war game as a web based system in a fastest way without affecting the security level. From the experimental results the proposed EEVPN is faster with losing to the security level.

The proposed EEVPN is more effective because it is faster than other VPNs in sending small data size; where it takes small data transmission time, achieving high level of security. Also, the proposed EEVPN is more extensive because it is not built for a specific environment, which makes the customization of the VPN is very difficult, so it can be installed at any environment which is faster and more secured than many other VPNs like CISCO VPN and IBM VPN incase of transmitting small data size (*i.e.* less than 1 MB).

We plan in the near future to implement some techniques in order to enhance quality of streaming over VPN.

6. References

[1] D. L. Clark, “IT Manger’s Guide to Virtual Private Networks,” McGraw-Hill, New York, 1999.

[2] S. Badr, “Security Architecture for Internet Protocols,”

Ph.D. Thesis, Military Technical College, Cairo, 2001.

[3] A. Farouk, "Intrusion Detection in a War a Game Web Based Application," Master of Science Thesis, Ain Shams University, Cairo, 2004.

[4] A. E. Taha, "Secured Access Control in Web Based War Game Application," Master of Science Thesis, Ain -Shams University, Cairo, Egypt, October 2002.

[5] N. Malheiros, E. Madeira, F. L. Verdi and M. Magalhaesb, "Managing Layer 1 VPN Services," *Optical Switching and Networking*, Vol. 5, No. 4, 2008, pp. 196-218. doi:10.1016/j.osn.2008.02.002

[6] P. Juste, D. Wolinsky, P. Boykin, M. Covington and R. Figueiredo, "SocialVPN: Enabling Wide-Area Collaboration with Integrated Social and Overlay Networks," *Computer Networks*, Vol. 54, No. 12, August 2010, pp. 1926-1938. doi:10.1016/j.comnet.2009.11.019

[7] A. G. Yay1ml1, "Selective Survivability with Disjoint Nodes and Disjoint Lightpaths for Layer 1 VPN," *Optical Switching and Networking*, Vol. 6, No. 1, 2009, pp. 3-9. doi:10.1016/j.osn.2008.05.002

[8] C. Xenakis, C. Ntantogian and I. Stavrakakis, "A Networkassisted Mobile VPN for Securing Users Data in UMTS," *Computer Communications*, Vol. 31, No. 14, 2008, pp. 3315-3327. doi:10.1016/j.comcom.2008.05.018

[9] M. N. Ismail and M. T. Ismail, "Analyzing of Virtual Private Network over Open Source Application and Hardware Device Performance," *European Journal of Scientific Research*, Vol. 28, No. 2, 2009, pp: 215-226.

[10] R. Bolla, R. Bruschi, F. Davoli and M. Repetto, "Hybrid Optimization for QoS Control in IP Virtual Private Networks," *Computer Networks*, Vol. 52, No. 3, 2008, pp. 563-580. doi:10.1016/j.comnet.2007.10.006

[11] S. Gold, "Pirate Bay Develops Anonymous VPN User Protection," *Infosecurity*, Vol. 6, No. 3, 2009, pp. 8. doi:10.1016/S1754-4548(09)70045-2

[12] D. Forte *et al*., "SSL VPN and Return on Investment: A Possible Combination," *Network Security*, Vol. 10, No. 10, 2009, pp. 17-19. doi:10.1016/S1353-4858(09)70112-6

[13] T. Rowan, "VPN Technology: IPSEC vs SSL," *Network Security*, Vol. 2007, No. 12, December 2007, pp. 13-17. doi: 10.1016/S1353-4858(07)70104-6

[14] J. F. Dunnigan, "Wargames Handbook: How to Play and Design Commercial and Professional Wargames," Writer's Club Press, 2000.

[15] Y. Dakroury, I. A. El-ghafar and A. Taha, "Secured Web-Based War Game Application Using Combined Smart Certificate and Secure Cookies Techniques," *Proceeding of the* 1*st IEEE International Symposium on Signal Processing and Information Technology*, Cairo, December 2001, pp. 447-453.

[16] Downloading rpm's for VPN, http://sourceforge.net/projects

[17] G. F. Luger, "Artificial Intelligence Structures and Strategies for Complex Problem Solving," 4th Edition, Addison Wesley, New York, 2001.

[18] K. Heller, K. Svore, A. Keromytis and S. Stolfo, "One Class Support Vector Machines for Detecting Anomalous Window Registry Accesses," 3*rd IEEE Conference and Data Mining Workshop on Data Mining for Computer Security*, Florida, November 2003.

