Performance Evaluation and Design Considerations of Ultra Virtual Private Network

A.Yashwanth Reddy
Assistant Professor, Sree Dattha Group of Institutions, Hyderabad, Telangana, India.

C.Swathi
Assistant Professor, Sree Dattha Group of Institutions, Hyderabad, Telangana, India.

R.Kalavathi
Assistant Professor, Sree Dattha Group of Institutions, Hyderabad, Telangana, India.

Abstract – A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network. Applications running across the VPN may therefore benefit from the functionality, security, and management of the private network. In other words a VPN can transform the characteristics of a public which may be non-secure network into private secure network through using encrypted channel or tunnel. The proposed solution is customized into a standard VPN called ULTRA VPN. It transmits a small data size through a web based system in a reasonable or optimized time without affecting the security level. The proposed ULTRA VPN is considered to be more effective as it takes small data transmission time with achieving high level of security.

Index Terms – ULTRA VPN, secure data transmission, virtual private network and private secure network.

1. INTRODUCTION

VPNs may allow employees to securely access a corporate intranet while located outside the office. They are used to securely connect geographically separated offices of an organization, creating one cohesive network. Individual Internet users may secure their wireless transactions with a VPN, to circumvent geo-restrictions and censorship, or to connect to proxy servers for the purpose of protecting personal identity and location. However, some Internet sites block access to known VPN technology to prevent the circumvention of their geo-restrictions [1-3].

A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. A VPN available from the public Internet can provide some of the benefits of a wide area network (WAN) [4]. From a user perspective, the resources available within the private network can be accessed remotely. Traditional VPNs are characterized by a point-to-point topology, and they do not tend to support or connect broadcast domains, so services such as Microsoft Windows NetBIOS may not be fully supported or work as they would on a local area network (LAN). Designers have developed VPN variants, such as Virtual Private LAN Service (VPLS), and layer-2 tunneling protocols, to overcome this limitation. A VPN uses data encryption to prevent unauthorized users from accessing data or information, and also ensures that data is not modified as it flows through the Internet. VPN uses the tunneling or channeling process to transport the encrypted and secured data across the Internet. Tunneling is a mechanism for encapsulating one protocol in another protocol. Early data networks allowed VPN-style remote connectivity through dial-up modem or through leased line connections utilizing Frame Relay and Asynchronous Transfer Mode (ATM) virtual circuits, provisioned through a network owned and operated by telecommunication carriers. These networks are not considered true [5-7] VPNs because they passively secure the data being transmitted by the creation of logical data streams. They have been replaced by VPNs based on IP and IP/Multi-protocol Label Switching (MPLS) Networks, due to significant cost-reductions and increased bandwidth provided by new technologies such as Digital Subscriber Line (DSL) and fiber-optic networks.

VPNs can be either remote-access (connecting a computer to a network) or site-to-site (connecting two networks). In a corporate setting, remote-access VPNs allow employees to access their company's intranet from home or while travelling outside the office and site-to-site VPNs allow employees in geographically disparate offices to share one cohesive virtual network. A VPN can also be used to interconnect two similar networks over a dissimilar middle network; for example, two IPv6 networks over an IPv4 network.

VPN systems may be classified by:

- The protocols used to tunnel the traffic
- The tunnel's termination point location, e.g., on the

customer edge or network-provider edge

- The type of topology of connections, such as site-to-site or network-to-network
- The levels of security provided
- The OSI layer they present to the connecting network, such as Layer 2 circuits or Layer 3 network connectivity
- The number of simultaneous connections

A VPN consists of four main components: 1) VPN protocol, 2) Tunnel terminating device or VPN server, 3) Network Access Server (NAS), 4) a VPN client. In a VPN connection, a remote user (or VPN client) access a PPP connection with the ISP's NAS through public switched telephone network (PSTN). NAS is a device that is used to terminate dial-up calls over analog (basic telephone service) or digital (ISDN) circuits. The NAS is owned by ISP, and is usually implemented in the ISP's POP. Once the user is authenticated through appropriate authentication method, the NAS directs the packet to the tunnel that connects both the NAS and the VPN server.

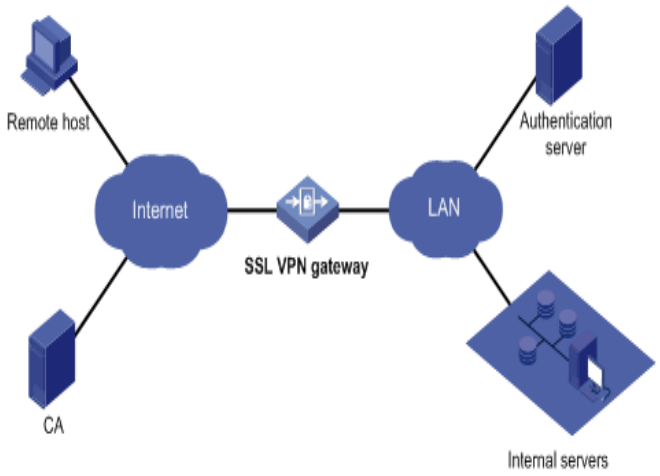

Figure 1. VPN Implementation

The VPN server helps us to recover the packet data from the tunnel, opens it, and delivers it to the corporate office network. There are four tunneling protocols used to establish VPNs, and three are extensions of the Point- to- Point Protocol (PPP) 1) Layer 2 Forwarding (L2F). 2) Point-to - Point Tunneling Protocol (PPTP. 3) IP Security (IPsec) Protocol Suite 4) Layer 2 Tunneling Protocol (L2TP). Let's also focus on IPsec with some details. Internet protocol security (**IPsec**) is a set of protocols that provides security for an Internet Protocol. It can use cryptography to provide security. **IPsec** can be used for the setting up of virtual private networks (VPNs) in a secure manner.

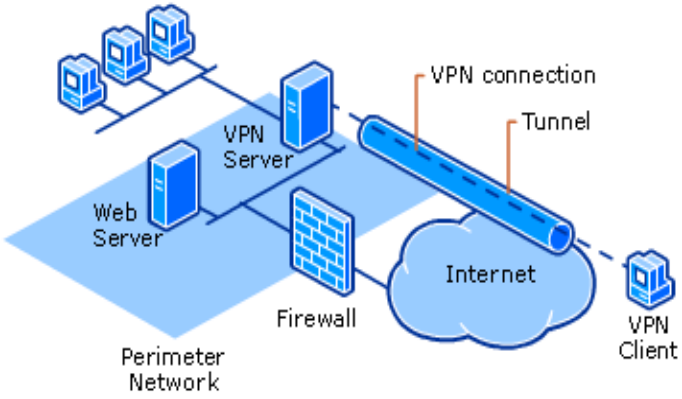

Figure 2. VPN Architecture

IPsec provides cryptography based protection of all data at the IP layer of the communications stack. It pro- vides secure communications transparently, with no changes required to existing applications.

IPsec protects network traffic data in three ways Authentication:

1) The process or action of proving or showing something to be true, genuine, or valid

2) Integrity checking: The process of comparing the current state of stored data and/or programs to a previously recorded state in order to detect any changes

3) Encryption: The process of converting information or data into a code, especially to prevent unauthorized access.

2. MARKETABLE VPNS

Many companies produced a lot of VPNs deals with different data sizes. On the other hand a few applications that deals with small data sizes which are less than 1 MB such as Race Game which needs high security with low time transmission. Let us discuss the most popular VPN commercial products Cisco VPN. VPN products from Cisco Cisco's Cisco VPN client 3.0, Cisco Easy, VPN 3000 Concentrator. E Token, lets us access only one password to remember. Users can take their authentication keys and digital certificates with them and access whenever they want wherever they go, on a key chain. 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. Cisco Easy VPN is cisco software that enhances the existing Cisco routers and security appliances. It simplifies VPN deployment for remote offices and teleworkers.

Based on the Cisco Unified Client Framework, Cisco Easy VPN helps in centralization of all Cisco VPN devices reducing the complexity of VPN deployments as per the given cisco information. Cisco Easy VPN enables an

integration of VPN re- motes-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 as per cisco given information.

Race game is a simulated race between two or more opposing racing sides. There are two race sides and they are represented by the red and black colors. Each car has its own check points to achieve at the expense of the other side, considering each side capabilities, rpm, and Racing experience during the race. In addition, environmental conditions also play a vital role such as race tracks or terrain nature, race timing, weather etc. In addition to the racing sides, one more side representing the mediator must be existed in the race game system.

The mediator side is responsible of monitoring the racing sides and evaluates their decisions. Although it may be possible to play some forms of race games without the use of any prepared materials, most race games require a set of tactics to keep track of and display data, force locations and movements, and interactions between different racing units. We have different instrumentality of race games. Manual games, which represented by simple tools: maps, charts, notebook of data, and orders of race, although 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 race positions, their movement, racing capabilities, and other critical, data-intensive pieces of information.

The integrated software components for implementing web based race games system of each side include: 1) Operating system component 2) Database component 3) GIS component. Securing web based race games system is very important. The main aim is to achieve a high level of security to the web based race game system and controlling its sides' behaviors. Since the entire network packets are going from or to the side LAN should be passed through the gateway computer, the security process is activated on the gateway computer.

3. PROPOSED MODEL AND RESULTS

The proposed model provide three levels of security to secure the web based race game system in the following procedure as shown in figure 3. The access control is applied to our web based race game system using two access control mechanism structure. The first mechanism is the server operating system access control mechanism. This mechanism is applied to the race game system resources (directories, files etc). The second mechanism system is the DBMS access control mechanism and it is applied to the race game system database. Virtual Private Network security module is responsible for performing two important tasks. The first task is to encrypt each network packet before going out from the side LAN to the web. The second task is to decrypt each network packet coming from the web before entering the side LAN. Intrusion detection & prevention module is responsible for checking and tracking each and every incoming network packet and testing 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 the information is given to the system administrator or the system admin and the packet is blocked.

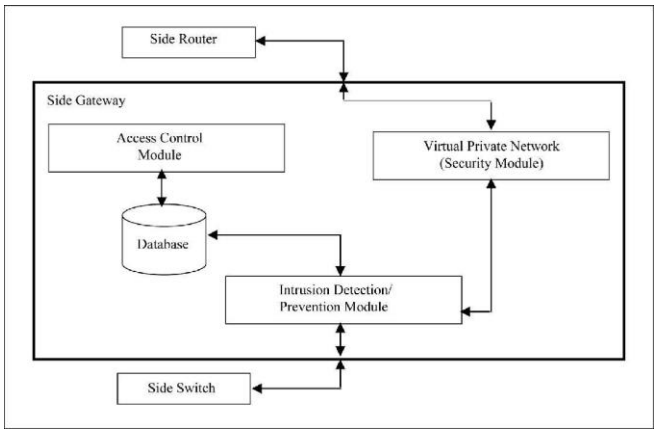

Figure 3. Security levels using a VPN

Some encryption schemes or plans are proven to be secure on the basis of past mathematical problem. Sometimes the secure encryption schemes has its own mathematical meaning, and there are multiple different other meanings or definitions. The proposed model use a public key cryptography taken from encryption schemes of VPN but used within our context in which the scheme will be deployed securely and safely as shown in fig 3. We have customized both PPTP and IP Sec for our ULTRA VPN by erasing or eliminating many overheads from them by considering only those which are needed for keeping security at large transmission time so that the transmission is faster without affecting security. ULTRAVPN is very easy to modify, install and operate. It is basically a wrapper for sending packets over an SSL connection. It supports public key encryption by using client & server certificates (SSLv3). Each layer of protocol adds some bytes of overhead. ULTRA VPN acts like a wrapper program to send packets over an SSL connection, no overhead is introduced by the ULTRA VPN program. However the underlying SSL layer does add some headers. ULTRA VPN does not support any compression or procedures. We conducted and analyzed a series of experiments with random packet sizes and measured the packet length on the wire. The experimental results one can conclude that ULTRA VPN solution adds an average of 157 bytes of overhead to the data.

ULTRA VPN uses the cryptographic functions provided by your SSL implementation plugin. Hence, if someone needs to add his or her own algorithm, he or she has to look for plugin support in the SSL implementation that he or she is using to build his or her own code or 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

Here the proposed ULTRA VPN algorithm is embedded in a race game system as a web based system to be one of the defense lines for securing the race game data over the public network. [We used Microsoft visual basic 6.0 enterprise edition to design and execute the security test program]

Test	Protocol	Bytes (KB	Bandwidth (Mbps)
1	TCP	1120	9.0
(non-encrypted wired)	UDP	1000	8.6
2	TCP	1110	9.0
(encrypted wired)	UDP	810	7.2
3	TCP	400	3.0
(non-encrypted wireless)	UDP	530	4.1
4	TCP	440	3.8
(encrypted wireless)	UDP	350	3.1

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 the hackers to access the data, modify it or even destroy it.

The transmitted data received at the destination side should have the capability to decrypt the data and understand it, otherwise it will not be able to understand the data if VPN decryption mechanism is not used.

4. CONCLUSION

A virtual private network (VPN) is a network that is constructed using public wires, usually the Internet, to connect remote users or regional offices to a company's private, internal network. Our customized standard Virtual Private Net-works (VPN) to a newly one called PROPOSED VPN. In fact we need to transmit a small data size in our example race game as a web based system in order to in fastest way without affecting the security level. From the experimental results the proposed VPN is an faster. The proposed VPN is more effective because it is faster than other VPNs in sending small data size; where it takes very less data transmission time. It has a achieving high level of security. Also, the proposed an VPN is more effective and efficient because it is no built for particular environment, so it can be installs at any environment which is faster and more secured a than many other VPNs like CISCO VPN in case of a transmitting small data (size less than 1 MB).

REFERENCES

[1] Mason, Andrew G. (2002). Cisco Secure Virtual Private Network. Cisco Press. p.7.
[2] Microsoft TechNet. "Virtual Private Networking: An Overview".
[3] Cisco Systems, et al. Internet working Technologies Handbook, Third Edition. Cisco Press, 2000, p.232.
[4] Lewis, Mark. Comparing, Designing and Deploying VPNs. Cisco Press, 2006, p.5.
[5] International Engineering Consortium. Digital Subscriber Line 2001. Intl. Engineering Consortium, 2001, p.40.
[6] Technet Lab. "IPv6 traffic over VPN connections". Archived from the original on 15 June 2012.
[7] RFC 6434, "IPv6 Node Requirements", E. Jankiewicz, J. Loughney, T. Narten (December 2016).