Intrusion Prevention System in VPN with Entities Based Access Rule and Vibrant Key Authentication.

G. Kanimozhi, S. Ravimaran, and M. A. Maluk Mohamed

***Abstract*—VPN technology continues to struggle with intruders attacks that cripple their network performance and connectivity. This compels security threats on the remote network because its firewall does not know what transfer is flowing within VPN tunnel. This paper proposes a new framework called V-Safe which provides vibrant key authentication and entities based access rule to prevent intruders. The traditional access rule models are group based and it is not an effective mechanism since it uses common identity for access control. The entities based access rule provides access permission based on various entities like requestors, resources, actions and environment that will prevent against intruders and performs deep scans to detect and block most suspicious threats and attacks. The V-Safe framework is evaluated through simulation and it shows the proposed system is more secure and efficient than the existing intrusion prevention system.**

***Index Terms*—Virtual private network, intruders, authentication, IPsec, firewall.**

I. Introduction

Expansion of organizations globally requires secure electronic communications among physically distributed remote locations. Virtual Private Networks (VPNs) offer an economically feasible option to deal with this need. A VPN is a private network that uses the public Internet to connect remote users to the organization’s internal network. Since a VPN uses the Internet; it continues to struggle with intruders attacks that cripple their network performance and connectivity. VPN users will transfer sensitive data but the VPN needs additional security mechanisms like encryption, use of strong authentication and access control. Though the VPN tunnel is very useful for the organizations, it compels security threats on client’s network because client’s firewall does not know what transfer is flowing within the VPN tunnel. For example, even if client’s firewall blocks access to a remote site (say, www.intruders.com), it cannot enforce its policies on the server which belongs to the organization even if the system is physically on client’s network. Thus, the VPN tunnel opens a hole to client’s firewall that may allow unwanted traffic to flow in and out. This could destabilize VPN as intruders could flood in through it to the organizations sensitive server first and then further spread to other nodes on client’s network.

Many organizations configure their remote access VPN to allow full access to the internal network for VPN users. This means that if the VPN is compromised, then the attacker gets full access to the internal network too. Hence its vital role is to have the high security VPN framework to ensure strong secure communication in VPN network. Thus this paper proposes a new framework called V-Safe which provides vibrant key authentication and entities based access rule to prevent intruders. Using a single factor static password authentication alone is not enough to secure the VPN from the unauthorized users. Henceforth, this V-Safe provides strong and secure authentication system called vibrant key authentication system. This yields dynamic key credentials to the users through their mobile phones. Additionally access control model has to be improved. Entities based access rule provides access permission based on various entities like requestors, resources, actions and environment that will prevent against intruders and this Intrusion Prevention System for VPN is an approach based on the provision of a dedicated security, called V-Safe, that automatically manages tunnel requests coming from the users.

The motivation is to increase the security level of tunnels configurations. This technique can blacklist misbehaving users while maintaining their privacy, and show how these properties can be attained in a way that is practical, efficient, and sensitive to the needs of both users and services. By using V-Safe framework, organizations can enable the secure remote access to their networks through VPN technology. The solution will make organizations of all sizes and complexities extend the reach of extranets to remote employee’s in-line with organization’s business strategy. The rest of this paper is organized as follows: Section 2 presents Background and related work in VPN security, Section 3 describes proposed V-Safe framework and Section 4 provides Performance Evaluation, finally Section 5 draws Conclusion of this paper.

II. Background and Related Work

In this section, several existing security models for VPN that have influenced the proposed work are briefly discussed. VPN technology involves remote accessing, roaming users can enjoy the security protection offered by VPN and little consideration has been given to the impact of such encrypted tunnels on the server network. In particular, the server network's firewall cannot effectively regulate such tunneled traffic, because it is unable to examine the encrypted connection properties, such as destination IP addresses and ports. It is very difficult to regulate the encrypted tunnels

Manuscript received March 05, 2012; revised April 05, 2012.

G. Kanimozhi and S. Ravimaran are with Software System Group, Department of Computer Science and Engg.

M. A. M Mohamed is with M. A. M. College of Engineering, Anna University Tiruchirappalli, India (Corresponding author. Tel.: + 09965628881, fax: + 914312650377, e-mail address: ssg_kanimozhi@mamce.org).

using conventional firewall techniques [1]. To understand the application of VPN there is an e-learning platform which is based on VPN technology in order to ensure the secure document transfers and communications for online teaching courses in [2].

The common type of security attacks and risks in VPN are in [3]. To increase security it is necessary to regularly upgrade VPN security system by means of a newer firewall which has additional protection functions [4].Basically, to early prediction and prevention suspicious threat, there are two approaches, Host-based approach and Network-based approach [5][6].Signature is primary factor in intrusion prevention, which identify something and stops it. This must be distinct characteristics. Signature triggers, using trigger action which can be applied atomic and stateful signature [5],[7],[8]. Another issue of IPS is traffic volume, if the bandwidth increases then the traffic monitor will affect the overall utilizing performance [9].

Network Authentication, Authorization, and Accounting (AAA, pronounced "triple-A") is a technology that has been widely used. It is important to understand the roles played in the AAA System [10]. VPN mainly adopts four technologies to guarantee security, respectively tunneling, encryption and decryption, key management, and authentication [11]. As a direct means of logical authentication, though, the reliance of human being on another has little supporting scientific literature or practice [12]. Although, VPN technology ensure the privacy of data transmission over public domain by creating an encrypted “tunnel” through the public network , but does not strongly protect unauthorized access to the organization’s assets. This happens because simple username and password is used to protect the access to most VPN s. So, information that is secure while in transit may just be ending up in the wrong hands at its final destination. Security experts worldwide suggest the usage of a strong, two-factor authentication to protect remote access [13].

About access control for VPN, Jason et al. [14] presented an object-oriented information model of IPSec policy designed to facilitate agreement on the content and semantics of IPSec policy, and to control actual task. Generalized Role-Based Access Control Model (GRBAC) [15]. GRBAC is highly expressive and easy-to-use access control model. VPN usually means sensitive information for hackers; therefore a VPN needs to go through a thorough penetration test to check for vulnerabilities [16]. The permissions to carry out definite operations are assigned to precise roles [17]. The enhancement to role-based access control by introducing the domains that flexibly partition access control scope and exceed the limit of the organization frame. And, the domains fix the restrictions that can be added to the traditional concept of permissions in order to keep the number of permissions small [18]. Compared with these researches, V-Safe framework emphasizes more secure VPN by preventing from being smashed before threats arriving.

III. Proposed V-Safe Framework

VPN technology continues to struggle with intruders attacks that cripple their network performance and connectivity. This compels security threats on the remote network because its firewall does not know what transfer is flowing within VPN tunnel. This paper proposes a new framework called V-Safe.

A. *Overview of System Architecture*

V-Safe purpose is to safe guard the VPN from the intruders and to avoid the security flaws existing in it. The overall system architecture as shown in the fig 1; Before the VPN tunnel establishment the authentication process has to be done in order to secure the IP of the VPN server. The pseudo code for the authentication process is shown in the table 1.

TABLE I: Pseudo Code for Vibrant Key Authentication

```
//User Registration with Secure web server
Read  User Information(Uname, pass );
Get  net_details(IPadd,Port);
//Verify the User name in DB already
Exists or not then set flag
for (i=0;i<record length in DB; i++)
If (flag==false)
//Create account with basic properties
Else // Give alert message Try  Registration again.
//Login to get Authenticate
Get Login (Uname,Pass);
//Verify the username and  password  in DB
If(Uname,Pass exists in DB)
Then //Checks user with assigned IP
If (UserReqIP!= RegIP(username))
Give error message(“you are not authenticated user”);
Else Gen_Random no();
Rkey=Return(Random(x,y));
Add(Rkey, Time of Expiration);
Send(Rkey,IP address, Username);
Get(Rkey from User);
Validate user input(Rkey);
If(RKey=true)
Create Connection ();
Else Disconnect();
```

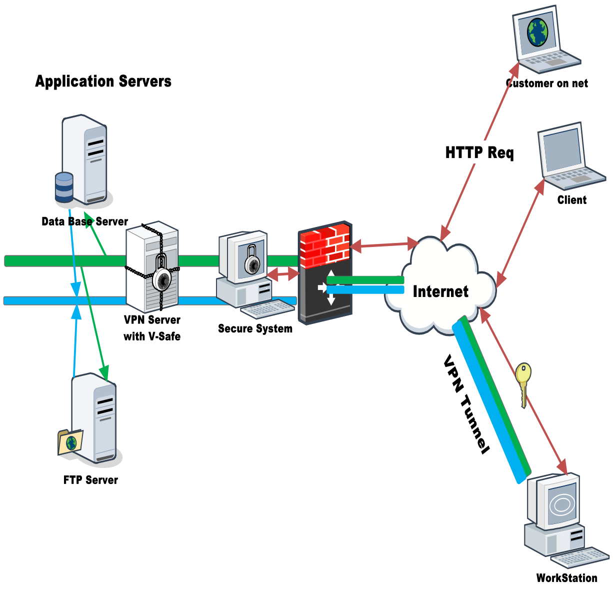

Fig. 1. System architecture

After the registration process, the user can login with the first level vibrant key authentication, which consists of one traditional static password, and then Secure System validates the user credentials and sends the dynamic key to the authorized user’s mobile device which is used within the expiry time of that key. These transfers are done by the regular web service using HTTP protocol through the public network. The Credentials are passed securely by using Message Authentication Code. Apply the IPSec protocol which is used to create the Virtual Private Network connection between the client and server. IPSec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of security gateways (network-to-network).Next to this, the VPN server with V-Safe frame work which is a new framework used for the VPN Secure access.

B. Functionality of V-Safe

The V-Safe Framework provides the creation of secured tunnel between the client and VPN server which includes the firewall policies of the client and server system, by non-overlapped rules of tunnel data transformation. This process involves packet filtering method inside the tunnel to yield a secure VPN service. The problem of preventing intruders entering into the VPN and the security attacks are termed as VPN intrusion prevention, as shown in fig 2 V-Safe framework.

The incoming packets are captured by the help of PCAP application program interface (Packet Capture API) for reading the packet flow of the tunnel and decrypted it, the captured packet will be analyzed and filtered which involves the rule manager in the V-Safe that is derived from the existing firewall, that include the IP validation, Packet Filtering Protocol and Port Identification to check for intruders and misbehaving service, is requested or not.

Furthermore the secure server does the monitoring process and validates whether the rule is applied for the particular user or not. VPN users has access to the various remote resources, it should give proper accessing rights to the legitimate user in order to provide privacy to the resources and services. The traditional access rule models that are role based are not effective since it uses common identity for access control.

V-Safe has entities based access rule, each user is unique and has a different combination of access permission depends on entities like requestors, resources, actions and environment. So with this kind of access the user will always have the secured remote access, this Intrusion prevention System that scans deep to detect and block most suspicious threats and attacks by relying on information gathered by the secure- monitoring server they will protect and monitor the behavior of the users in the Virtual Private Network and block then and there if necessary.

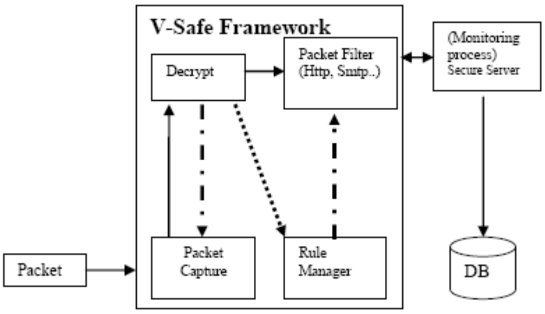
V-Safe Framework
Decrypt
Packet Filter (Http, Smtp..)
(Monitoring process) Secure Server
Packet
Packet Capture
Rule Manager
DB

Fig. 2. V-safe framework

IV. Performance Evaluations

VPN requires a deep understanding of public network security issues and proper deployment of precautions. The performance evaluation analysis of V-Safe framework with the properties of cost, network traffic, load balance and throughput is described below;

Cost Effective: Generally to solve the detection and fixing issue it is necessary to create the intrusion detection system. For timely detection, reaction and fixing of problem it involves a third party detector, but the V-Safe frame work has an own monitoring system to prevent the attacks and intruders.

Traffic Reduced: Normally the Intrusion Detection technique in VPN will trace the content flowing in the network or may monitor the router and intimate the server about the status of the intruder detection. But in V-Safe, the Intrusion Prevention System itself is doing the monitoring activity and prevents the intruders then and there where it is necessary. Henceforth, the network traffic is reduced obviously and the data throughput is increased.

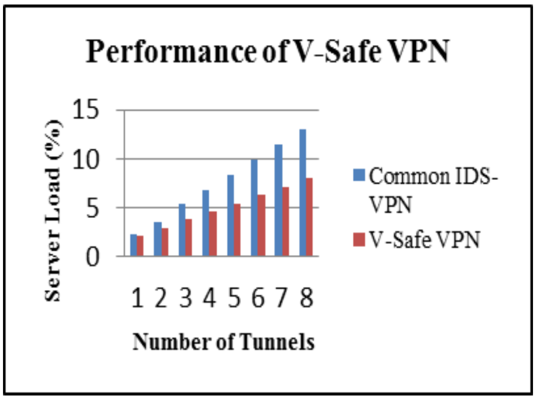

Fig. 3. Performance of v-safe VPN

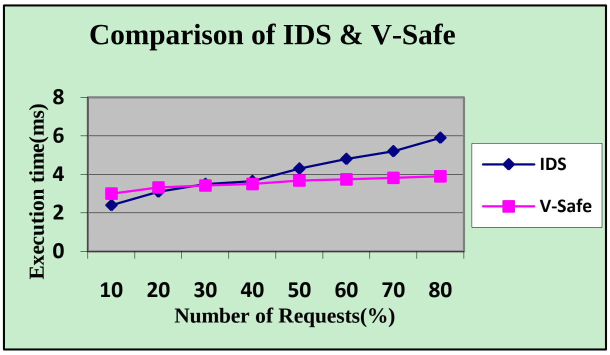

Fig. 4. Comparison of IDS and v-safe

Optimized Load Balance: The secure host system takes a process of authentication mechanism before the VPN connection is established then the VPN server V-Safe System will take over the connection establishment of the VPN, Henceforth sharing of process by the separate system, as shown in fig 3. This V-Safe framework provides the effective load balance to the Virtual Private network.

Comparison of IDS VPN and V-Safe VPN: When the number of requests increases in external existing Intrusion Detecting System then the execution time will be increased tremendously. But in V-Safe VPN though the number of requests increases the execution time will be maintaining better response as shown in the fig 4. Without fall in performance, results are obtained when compared to other existing IDS.

V. Conclusion

A VPN needs additional security enhanced features to protect the private network. Since the firewall does not know what transfer is flowing within VPN tunnel. This paper provides a new framework called V-Safe which yields vibrant key authentication to enable the initial level of strong secure authentication, before establishing the VPN connection. Furthermore the entities based access rule, which is based on various entities like requestors, resources, actions and environment prevents misuse of the critical resources and intruders. This system performs deep scans to detect and block most suspicious threats and attacks. To increase security in VPN it is necessary to regularly improve VPN security system by means of a newer firewall which has additional protection functions. Automatic blocking of misbehaving user and blocking of similar attacks is possible through improving the security system by means of a type of IPS (Intrusion Prevention System) called V-Safe. Moreover, this IPS provides the good performance then the existing Intrusion Detection System and also provides increased throughput, reduction in network traffic, cost effective and achieved optimized load balance. Using V-Safe framework, organizations can enable the secure remote access to their networks through VPN technology with stronger security and better performance.

References

[1] J. Cheng, H. Yang, S. H. Y. Wong, P. Zerfos, and S. W. Lu, "Design and Implementation of Cross Domain Cooperative Firewall," *Network Protocols, IEEE International Conference (ICNP 2007)* Oct 2007, pp. 284-293. 2007.

[2] I. Lita, S. Nicolaescu, and D. A. Visan, "VPN Platform for E-Learning Technologies Focused On Group of Topics: Passive Components and Circuits Electronic Materials, Electronic Technology," *Electronics Technology (ISSE) 34th International Spring Seminar.* May 11-15 2011, pp. 655-659. 2011.

[3] Steven Song, "SSL VPN Security," http://www.cisco.com/web/about/security/intelligence /05_08_ SSL VPN Security.html *Cisco press* 2008.

[4] I. Fosic, O. Sijiek, D. H. Osijek, and D. C. Zagar, "VPN Network Protection by IDS system Implementation," *MIPRO, Proceedings of the 34th International Convention,* May 23-27, 2011, pp. 1480-1484. 2011.

[5] E. Carter, et aI, "Intrusion Prevention Fundamentals: an introduction to network attack mitigation with IPS," *Cisco press,* 2006.

[6] M. Ahmed, R. Pal, M. M. Hossain, M. A. N. Bikas, and M. K. Hasan, "NIDS: A Network Based Approach to Intrusion Detection and Prevention," *International Association of Computer Science and Information Technology - Spring Conference,* April 17-20, 2009, pp. 141-144. 2009.

[7] C. M. Akujuobi, N. K Ampah, M. N. O Sadiku, "Application of Wavelets and Self-similarity to Enterprise Network Intrusion Detection and Prevention Systems," *Consumer Electronics IEEE International Symposium (ISCE) ,* June 20-23 2007, pp. 1-6. 2007.

[8] K. Haslum, M. E. G. Moe, and S. J. Knapskog, "Real-time Intrusion Prevention and Security of Network using HMMs," *Local Computer Networks (LCN) 33rd IEEE Conference,* October 14-17, 2008, pp. 927-937. 2008.

[9] D. Stiawan, A. H. Abdullah, and M. Y. Idris, "The Trends of Intrusion Prevention System Network," *Education Technology and Computer (ICETC) 2nd International Conference,* June 22-24, 2010, pp. v4 217-v4 221. 2010.

[10] Sean Convery, "Network Authentication, Authorization and Accounting," *The Internet protocol Journal* vol. 10, no. 1, March 2007.

[11] X. M. Bai, F. Zhang, and D. Wang, "The Application of VPN Technology in the University's Library," *Communication Software and Network (ICCSN), IEEE 3rd International Conference,* May 27-29, 2011, pp. 563-566. 2011.

[12] B. A. Juels, R. L. Rivest, M. Szydlo, and M. Yung, "Fourth-Factor Authentication: Somebody You Know," CCS'06 *proceedings of the 13th ACM Conference on Computer and Communication Security*, pp. 168-178, 2006.

[13] Arraysheild [Online]. Available:http://www.arrayshield.com/uploads/ArrayShield-Technical Synopsis-VPN.pdf Arraysheild Private Limited.

[14] J. Jason, L. Rafalow, and E. Vyncke, "IPsec Configuration Policy Information Model," *The Internet Society August 2003, RFC3585.* 2003.

[15] M. J. Moyer and M. Ahamad, "Generalized role based access control," *Distributed Computing systems, 21st International Conference,* April 2001, pp. 391-398. 2001.

[16] T. K. Shih, "Advanced Penetration Testing Methodology for VPN," *Journal of Security* 2008, pp. 419-424.

[17] S. Ahmad and R. Ahmad, "Design of Algorithm for Environment Based Dynamic Access Control Model for Database Systems," *International Journal of computer application, published by Founder of computer science,* May 2011,vol. 21, no.10, pp. 1-8. 2011.

[18] H. Zhao, Z. Fang, and L. Shi, D. Zhao, and J. Univ, "Domain-Based Access Control for Collaborative E- Commerce System," *Pervasive Computing and Application ICPCA*, July 26-27, 2007, pp. 162-167.