

SPS-VN: Research on the Security Policy System for Virtual Network

Guannan Gong, Liang Hu, Kuo Zhao, Jinxin He, Yuefeng Xu, Ying Duan
Department of Computer Science and Technology
Jilin University
Changchun City, Jilin Province, P.R.China

Abstract - *In the area of network information security, it is necessary to study the security in the end-to-end communication. This paper proposes a theory of virtual network by end-to-end. By researching the IPSec, security policy system and the technique of virtual network, it combines them together to design a framework of virtual network prototype system, and introduces the key technique and implement.*

Keywords: IPSec, virtual network, security policy system, security domain, work group

1 Introduction

As construction of information develops, application of every kind of network is spread and popularized. The importance of information security is regarded by more and more trade and user. Currently, the most general network information products and solving methods are faced to trans-enterprise network and wide-area network. The basic unit protected is enterprise network. The direct theory is uniform disposition from system to network and to application layer, solving the security problems in system and network layer using firewall, intrusion detection and antivirus product. Centralize security service platform to finish ID verification, authorization and encrypt-transport of data, thus the problems in application layer are solved. The technique of VPN [1] develops and grows up, it solves three different kinds of security communication problem: (1) Between each department of enterprise and remote branch—Internet VPN; (2) Remote access between enterprise-network and remote (mobile) employee—(Remote Access) VPN; (3) Extranet VPN between enterprise and partner/client/provider. That makes actualization granularity of network security settlement more and more detailed.

Security consciousness of client power proposes many more new problems in area of network information security. In the area of network security, there is one problem not often referred which is the security among host computer (or client) of enterprise network. The traditional conception is an assumption that the intranet is secure, but actually it is unlike people's imagination. With analyzing a great deal statistic information of network attack, the attack to key service and sensitive data of

enterprise network have the great proportion, but there is no effective study and solution for it.

Inside of enterprise network, it is different in security request of network because it is different in service and security concern of every client. The insecurity of IP network result in that it is impossible to transport data on unreliable network among members of security department, security departments need to in security separate from other department. This scene is common in actual environment, maybe it could be separated in data link layer and network layer by using equipments and administrator configuration, but it would lose sensitiveness and operability. Personal firewall can help host computer resisting network attack and in-break, but it cannot solve the problems of security access and encryption transport. We analyze that there are three disadvantages in current solution of network security:

- (1) Disable to solve the security problem of communication among host computer (client) inside enterprise network.
- (2) Need to add hardware equipment and adjust network architecture if increasing security.
- (3) After increasing security disposition, opaque for client, the application system would change.

VPN technique is based on industrial standard and protocol. The protocols contains IPSec [2,3], Point-to-point Tunneling Protocol (PPTP) [4], Layer 2 Tunneling Protocol (L2TP) [4] and so on. IPSec protocol is a extensive and open security protocol of virtual private network (VPN). It is layer 3 tunneling protocol that finishes data packaging in network layer, offers protection to data above the network layer and transparent security transfer. IPSec ensure the security of data by encryption technique from three fields as follow.

- (1) Verification. Using for ID authentication of host computer and terminal.
- (2) Integrity. Using for ensure that the data is not modified during network transport.
- (3) Encryption. Ensuring private by encrypting IP address and data.

After our analysis, under the environment of inside enterprise network and cross-enterprise network, combining with security policy system, we consider that there is a feasible way by adding some security character to IP protocol using IPSec technique, making virtual network

for client, and offering transparent security communication tunnel without any hardware equipment.

2 Security Policy System and Foundation of Virtual Network base on IPSec

2.1 Summary of Security Policy System

IPSec is one protocol cluster; it is an Internet security standard offering encryption, integrity and authentication service to information transferring in IP network. IPSec can add security character to IP layer, but it will not modify any application of higher layer. These security characters are defined by security policy. The policy is composed with a series of rule set; it is used for controlling different behavior of network under different environment. The network base on tactics can decide dynamic security protection measure for message from the character of client (communication entity). IPSec workgroup of IETF (Internet Engineering Task Force) [5,6] design a draft of Security Policy System (SPS) [7,8,9] and define the frame of SPS (shown in Fig.1), policy describing language and policy access form to the security policy problem. IPSec also add to network base on policy.

The definition of SPS use security domain as a unit. Security domain is the set of communicate entity and resource sharing a group of security policy database. Security Policy System is formed with five parts: SPS database, Policy server, Policy client, Security gateway and un-local domain policy system. SPS database defines resource and policy for accessing data of security domain. Policy server maintains SPS database and receive the request information from policy client and other policy server. Then it returns proper policy information under access controlling rules.

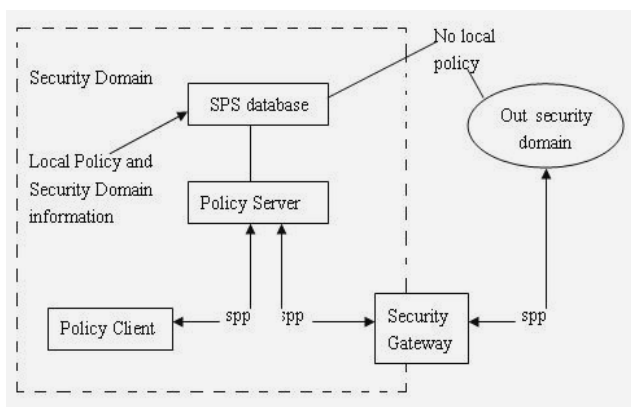


Fig. 1. Security System Model

Policy server and policy client exchange policy information by SPP, security gateways decide the bound of security domain. Security gateway, policy client and other domain server all could be regarded as policy clients, they

all can exchange information with local domain policy server. Security Policy Specification Language (SPSL) [10] is a language that is independence of provider and platform, it detailed explain the security policy that communication needs. SPSL allows using the common used language describing security policy, and store policy information into SPS database. The security policy and describing information of security domain are both detailed described by SPSL. The validity and integrity of policy in SPS is a hot problem, but it is not the main part of this paper.

2.2 Concept of Virtual Network

IPSec offers three kinds of security service: (host—host), (host—security gateway) and (security gateway—security gateway). The concept of virtual network we put award is referred to security policy system model, construct security domain inside campus network so much as cross-campus network. Divide clients in domain into Group according service relation, Group is a virtual concept that the clients of same office could belong to different workgroup but the clients from different office building could belong to same workgroup because of work property. From security character of policy constituted group, achieve IPSec protocol in network layer and offer transparent secure cooperated network environment to clients of virtual workgroup.

2.3 Connection of SPS and Virtual Network

The theory of end-to-end virtual network is embodied by SPS, security character (IPSec SA) is offered materials by security policy and arranged by IKE. The application of security character is achieved by packing IP message into IPSec message. Application of SPS in virtual network environment according to basic frame model of SPS, and discuss the detail groupware in frame. Change the academic model to realized model.

- (1) Description, organization and depositing of policy: referred to standard of SPSL language, describe communication entity and resource and security policy. Conformed to LDAP protocol [11], organize SPS database as directory tree and centralizedly store in LDAP database.
- (2) Unification of host policy and client policy: IPSec protocol is realized in network layer of OSI model, so atomic unit of IPSec policy is IP host. But concept of virtual network is base on Client, the minimal policy object is client. Achieve mapping between host and IP address by getting login IP address of client. Thus, the need of virtual network and IPSec could both be satisfied.
- (3) Security Policy Protocol (SPP): SPP is the protocol defined in SPS model that used for finishing exchange of policy information between policy server and policy client. Currently it is an universal protocol, we must

predigest the protocol for easy realization and use it to finish exchange of policy information.

According to security policy system model proposed by IPSec workgroup and actual need of application, we combine them organically and exploit an antitype system of end-to-end virtual network in a special application environment.

3 Realization of SPS under Virtual Network Environment

Currently, security among campus network is realized by using link encryption and network layer encryption. The realization of end-to-end virtual network (client to server, client to client) inside campus network and cross campus network, founding different end-to-end virtual network, could basically realize security isolation between different modes. The main frame of system is shown in Fig.2. End client always work on Windows Platform, so realization and development of the system is under Windows environment. Make the most of standard protocol and exploit environment that is foreign to platform when we realized the system, and sustain cross-platform application and disposition.

After analysis, building IPSec communication mechanism between host of end client need to achieve banding of IP protocol and IPSec in network communication layer according to protocol standard of IPSec. Building policy system model in application layer, achieve key auto-exchange and arrangement by IKE according to IPSec protocol standard. In the whole system frame, the foundation of policy model embodies theory of virtual network. In this paper, we mainly introduce the key module in designing and achievement of Policy System:

- (1) SPS Database: Introduce the concept of workgroup from concept of standard SPS database, define the clients who attend to research of same pattern and product researching is one workgroup. Manage security domain, workgroup, policy and client in the form of directory tree. Definition of Policy: the clients of same group share one group of security policies, force IPSec communication; it is forbidden to communicate among clients of different group; Communication of clients not in group still use IP not IPSec. SPS database organize the communication entity, resource and policy record as the standard of LDAP v3. And offer LDAP and API interface to access.
- (2) Policy Configuration Module: Offer interactive interface of policy modification, add in and delete to system administrator, and then send the result to policy server. Do policy configuration with group, because clients in the same group need one group policy only, clients in the group would communicate in same way of policy. The policy information configured in configuration

interface includes all parameters that the system needs.

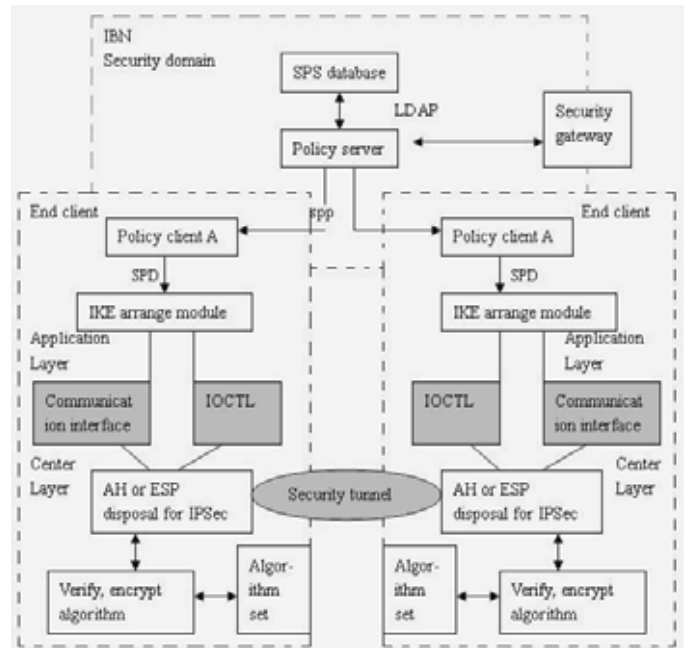


Fig. 2. System Main Frame structure

- (3) Policy Server: Work on policy server in the way of demon process. Doing centralized policy management, take charge checking of validity and integrity up the policy that policy configuration module get. Every workgroup define a group-spread address. When demon process receives the modification information, send policy-to-policy client in the way of group-cast.
- (4) Policy Client: Be in Windows system as a waiter. When refers to communication that policy set, finish client's login and catching the mapping relation between client and IP address. Get the group-cast information of the group from policy server, monitor modification of policy and startup IKE module at the same time. Change local SPD [12, 13] to IPSec SA, transport it to center layer through Windows I/O communication interface, and do IPSec message disposal by module of center layer network.

4 Conclusion

The IPSec achievement base on Security Policy System (SPS) offer a way in solving the network information security problem under the environment of end-to-end virtual network. As we have finished SPS under virtual network, we understand SPS in-depth and propose a consummate project to the system.

In SPS, before policy information exchange among communication entity is finished, the way of verification

could use Digital Signature of SPP or IPSec. There is some difficulties in achieving Digital Signature and IPSec, SPP not only is a provider but also is an user to IPSec, it is just like the relationship between "egg & chicken". The achievement of Digital Signature needs PKI [14] architecture's sustainment. In order to debase the complexity, improve security by SPP data message encryption in security domain. If refers to policy exchange that cross domain, Identity Verification among communication entity is the unavoidable problem. On the other hand, we can use manual and auto mode in policy configuration. Current system use manual mode, for extension of virtual network system, it should use auto-configuration. We can use for reference that discovery and spreading of routing information if we want to achieve SPS policy auto-discovered. In conclusion, the achievement of this system is an attempt that combines IPSec protocol in detail environment. We believe the system would be much better as knowledge of SPS consummates and standardizes.

References

- [1] David Andersen, Hari Balakshnan, Frans Kaashoek, and Robert Morris. Resilient Overlay Networks. Symposium on Operating Systems Principles, 2001.
- [2] Douglas Maughan, Mark Schertler. Internet Security Association and Key Management. Internet-Draft, Feb. 1996.
- [3] Charanjit S.Julia. Encryption Modes with Almost Free Message Integrity. Lecture Notes in Computer Science, 2000.
- [4] Niels Ferguson, Bruce Schneier. A Cryptographic Evaluation of IPSec. Preprint, Jan. 2000.
- [5] Van Jacobson. Congestion Avoidance and Control. In ACM SIGCOMM'88. 1988.
- [6] Henning Schulzrinne, Stephen Casner, Ron Frederick, and Van Jacobson. A Transport Protocol for Real-Time Applications. Internet-Draft, Oct. 2000.
- [7] L A Sanchez, M N Condell. Security Policy System[S]. Internet draft, Nov. 1998.
- [8] L A Sanchez, M N Condell. Security Policy System[S]. Internet draft, July. 1999.
- [9] M Condell, C Lynn, J Zao. Security Policy Specification Language[M]. March 2003.
- [10] Peiwei Mi, Walt Scacchi. A Knowledge based Environment for Modeling and Simulating Software Engineering Processes. IEEE Trans. On Knowledge and Data Engineering, Sept. 1990.
- [11] Rich Wolski, Neil T.Spring, Jim Hayes.The Network Weather Service: A Distributed Resource Performance Forecasting Service for Metacomputing. Future Generation Computer Systems, Oct. 1998.
- [12] S Kent, R Atkinson. Security Architecture for the Internet Protocol[S]. RFC 2401,Nov. 1998.
- [13] John Rushby. Using Model Checking to Help Discover Mode Confusions and Other Automation Surprises, HESSD, 1999.
- [14] Dan Boneh, Matthew Franklin. Identity-Based Encryption from the Weil Pairing. Extended abstract in Proc. of Crypto'2001.