Journal of Theoretical and Applied Information Technology
28th February 2013. Vol.48 No.3

ISSN: **1992-8645** www.jatit.org E-ISSN: **1817-3195**

STUDY AND IMPLEMENTATION OF LIBRARY WORKGROUP BASED ON SECURITY POLICY SYSTEM

[1]HE PING

[1]The library of Chengdu University of Information Technology Chengdu 610225

ABSTRACT

IPSec provides cryptographic-based security protection mechanism for IP packets. The correct implementation of IPSec depends on the security protection parameters included in security policies. IETF Library workgroup‘s proposal of security policy system architecture can simplify the task of managing security policies and ensure the proper deployment of security policies. By referring to this standard security policy system architecture, this article proposes a method of building a Library workgroup based on security policy system to distribute policies. The overall architecture of the library workgroup based on security policy system is given in combination with an end-to-end security communication prototype system. Finally this article discusses modules of the library workgroup based on security policy system and key techniques used in the system.

Keywords: *Ipsec; Security Policy System; Library Workgroup; Group Security Policy*

1. INTRODUCTION

With the rapid development of network communication technology, IP network has been playing an increasingly important role in the social and economic development. However, in order to apply this constantly updated network technology in the enterprise business, a very important factor to consider is how to protect data security in network communication effectively.

As a set of protocol standards for protection of IP packets, IPSec can be deployed in many kinds of network equipment that needs to establish a secure IP connection such as router, gateway and host. In addition to be able to provide access control protection the same to the firewall, IPSec can also provide data confidentiality, data integrity, authentication and anti-replay protection. So IPSec management is much more complex than the firewall. IPSec implementation is based on the correct configuration of the security policy that guides IPSec protect the communication data. But the traditional manual configuration method is inefficient and error-prone, especially in large-scale network environment, there will be a lot of problems.

The security policy system provides a solution to the security policy configuration through centralized deposit in the security policy server and automatic distribution to network equipments running the security policy client. This solution can simplify and speed up the security policy configuration process and can ensure the security policy configuration consistency. By taking reference to the security policy system framework proposed by IETF (Internet Engineering Task Force), in this article a LAN-based security policy system is proposed that is used in an end-to-end secure communication system.

2. IPSEC PROTOCOL AND LIBRARY WORKGROUP BASED ON SECURITY POLICY SYSTEM

2.1. Overview Of Ipsec Protocol

IPSec includes a set of open protocol standards proposed by IETF and now it has become IPV6 security standards and can also be applied to the current IPV4. IPSec protocol can be considered as a network layer protocols. As is known IP is the bottom layer of the entire end-to-end communication layers, but it did not consider security issues in the initial design. So IP cannot ensure the security of the high-level protocol payload, and therefore cannot ensure the security of data communication. Through encapsulation and protection of the IP layer data IPSec protocol can provides transparent and secure communication for upper protocol layer. IPSec uses cryptographic techniques to ensure the security of the data from the following aspects:

(1) Data encryption: Encrypting IP address and data to provide confidentiality.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

(2) Identity authentication: Authenticating hosts or security gateways on the other communication end.

(3) Integrity verification: Ensuring that the data transmitted over the network is not maliciously changed.

(4) Anti-replay protection: Preventing the legitimate communication packets from being sent repeatedly which may cause the leakage of information.

The IPSec protocol standards consist of three protocols: AH (Authentication Header), ESP (Encapsulating Security Payload) and IKE (Internet Key Exchange). The AH protocol ensures a reliable source of data and data integrity and provides protection measures to prevent message replay. ESP implements all the features of the AH and in addition it provides data encryption to payload. IKE is responsible for key exchange and negotiation of SA (Security Association). According to different configuration and security requirements, AH or ESP can be used independently or in combination for greater security.

2.2. Overview Of Security Policy System

IPSec security services are based on security policy which provides a set of rules for the implementation of IPSec. In order to solve problems in the security policy configuration and distribution, IETF IPSec Working Group proposes SPS (Security Policy System) framework in January 1999. SPS is a distributed system and provides a mechanism of discovering, accessing and disposing security policy information so that the host and the security gateway can establish a secure end-to-end communication path along multiple security gateways (Figure 1). SPS consists of policy server, policy client, and security gateway and policy database. In this system framework SPSL (Security Policy Specification Language) is used to describe the security policy format and SPP (Security Policy Protocol) to distribute the security policy.

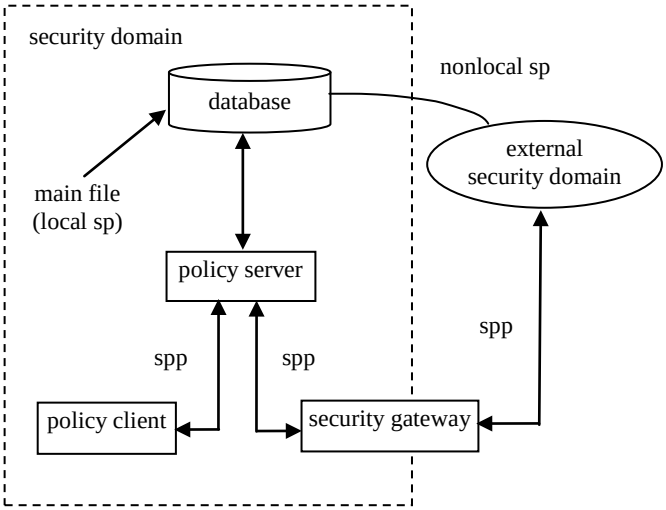

Figure 1 Sps Framework

In the security policy system framework proposed by IETF, configuration and management of security policy is based on the tunnel. The beginning and the end of the tunnel are all represented by IP address. Such tunnel-based security policy has the following drawbacks:

Poor scalability: Suppose N VPN entities need to build tunnels between each other, then the total tunnels to build is N (N-1) / 2. For tunnel-based IPSec VPN, both ends need to be configured. Therefore the total number of tunnel configuration times can reach to N (N-1). As N increases, the burden of tunnel configuration and maintenance can increase by complexity of O (N2).

Unreliable integrity: Network administrator often configures the tunnel according to intuition and experience, and there is no standard to measure the integrity of the whole security policy .If the tunnel is set up improperly, there will be loopholes or weak links. In addition, if tunnel configuration constantly changes, it is difficult to ensure that there is no redundant tunnel configuration.

Poor flexibility: There are often a lot of tunnel policies in large VPN network. If the network topology changed, it could cause extensive

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

modification of these tunnel policies. Because the tunnel configuration is based on IP address, VPN users using dial-up need to constantly change the tunnel configuration, which is clearly unacceptable.

Conceptually, SPS basically meets the demand of the IPSec policy framework proposed, but there are many problems in the implementation process. SPS provides good policy management thinking based on which we build a new type of security policy system.

2.3. Concept Of Library Workgroup And Group Security Policy

In this article, the concept of library workgroup is proposed which includes authorized users within the security domains. According to the business relationship those security domain users are divided into different library workgroups. The library workgroup is a virtual concept based on the division of labor. The same office users can be divided into different library workgroups, while different office users can be divided into the same library workgroup. The security is ensured by the security policy applied to the whole group which is called a group security policy.

Group security policy configuration is based on the following ideas: Users in the same library workgroup can make IPSec communication between each other. While users not in the same library workgroup are forbidden to visit each other so as to ensure that the library workgroup confidential data does not leak outside the group. Every library workgroup may include many users and the communication policy between the same group users is just the group security policy. So each security domain needs to deploy a policy server which is in charge of all the library workgroups, including group security policy and group users. And the policy server is responsible for the distribution of group security policy to each user in the library workgroup.

Definition of group security policy is a kind of user-based policy management strategy which is different from the original policy management strategy based on IP address. This policy management strategy has the following characteristics:

Strong scalability: In the library workgroup-based policy configuration, the policy number almost does not increase along with increment of the VPN entities. Each VPN entity is managed as an individual group user that does not affect the group security policy configuration and management. Compared with the tunnel-based policy configuration, group security policy configuration and maintenance burden only reach to complexity O (N).

Excellent integrity: For large VPN network using group security policy, the reasonable division of group can not only ensure the integrity of policy, but also eliminate the redundancy of policy.

High flexibility: When the network topology or the security requirement changes, the original policy can be easily modified to adapt to the change. At present, the mobile office has become a trend for many companies and organizations with VPN connection. In order to save money, they often setup a dial-up connection to the local ISP and then access the company's Intranet. The group security policy can be flexible to adapt to this IP address change.

2.4. Combination Of Ipsec And Library Workgroup Based On Security Policy System

The base of IPSec is SA which refers to a logical secure connection established between two communicating entities. A SA includes all the relevant information of IPSec protocol (AH or ESP) such as encryption algorithm, cryptographic key and the identity of communication parties. This security information is provided by the security policy, negotiated by IKE and finally applied to encapsulated IP packets to protect IP communication. In this article, the proposed group security policy system abides by the IPSec SPS framework, and the specific system modules of the framework are discussed as following.

Policy define and storage: The communication entities, resources and security policies in the security domain are properly defined by reference to policy RFCs and security policy documents as well as considering the specific application requirement. IETF provides a scheme to map the security policy to LDAP (Lightweight Directory Access Protocol) directory database. Taking into account the application environment is based on LAN environment with limited number of resource entities, so the relationship database is used to deposit library workgroup, user and group security policy data for convenience.

Group security policy translated to IP-based policy: IPSec protocol is implemented at the network layer and the traditional IPSec security policy configuration is based on the IP host, but the group security policy is a little different which is based on IP of the group user. In order to apply the group security policy to IPSec, the IP address of the clients

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

logged on need to be acquired to achieve translation from group security policy to IP-based policy.

Security policy distribution protocol: IETF has proposed a standard policy distribution protocol called COPS (Common Open Policy Service) which has two operating modes: passive mode and active mode. Passive mode means that the policy server responds to the policy request event from the policy client (IPSec devices) passively. The active mode refers to the server-side active distribution of policy to the client, for example the administrator sends command execution policy to the client. If the policy is stored in the form of an LDAP directory, you can also use the LDAP protocol to distribute the policy. Taking into account the specific application requirements, this article gives definition of an application layer communication protocol between the policy server and the policy client used to distribute the group security policy by reference to the COPS protocol. At the same time the policy server performs encryption on the distributing policy to ensure policy data confidentiality.

3. IMPLEMENTATION OF THE SECURITY POLICY SYSTEM

3.1. Architecture Of The Policy System

The security policy system has a three-tier architecture including client, server and database. A socket-based message communication method is used between the policy client and the policy server. The communication messages and the message format are defined according to the practical application requirements. The policy server deposits the security domain data such as library workgroups, library workgroup users and group security policies using a local relational database. Figure 2 is the architecture of a LAN-oriented end-to-end secure communication system which has three subsystems including the library workgroup-based policy subsystem, IKE negotiation subsystem and the IPSec Protocol implementation subsystem.

3.2. Description Of The Security Policy System Modules

The policy server provides services such as user state maintenance and group security policy distribution for all users in the security domain. And it also provides an interface for the security domain administrator to manage and configure the security domain data such as group security policy. When the administrator modifies the group security policy, the policy server will notify all the group users logged on to update the local group security policy data. Then all the users logged on begin to re-negotiate IPSec SA according to the new group security policy.

When the policy client logs on the policy server as a legitimate user identity of the security domain, the user will get the group security policy of its own library workgroup, and then the user will begin automatically to negotiate the communication IPSec SA through IKE negotiation subsystem with other users logged on in the same group. The C/S operation model reflects the thinking of library workgroup-based security policy management. This management approach has some advantages above.

The policy database uses the mature relational database system. The database structure is designed according to the application requirements mainly including some tables to save security domain data such as library workgroup, group user, group security policy and user state etc... The administrator can make a proper division of library workgroups based on application requirements. For example, if there are multiple project teams in the company, each project team can be considered as a library workgroup and the project team member can be considered as the library workgroup users. Sometimes one team member may take part in other project teams at the same time, and then the user can be put into multiple library workgroups.

3.3. Techniques Of The Security Policy System

3.3.1. Cross platform and cross network segment

The system implementation is based on the TCP / IP socket network communication technology. Because it is used in a local area network communication environment, the more efficient UDP protocol is used. And socket based communication interface can be well supported in different operating system platform, so the policy client can have the cross platform feature. Taking into account the possibility that the policy client and the policy server may not be on the same network segment, the system provides support for cross network segment. The policy server not only broadcasts messages to policy clients on the same LAN, but also uncast messages to theses clients in different network segment one by one.

Table 1 The Storage Mode Of Ontology Libraries

Name	WordNet	DBpedia	Cyc	HowNet
Storage mode	RCS	RDF triples	CFASL and HTML	Concept and Description

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

3.3.2 Definition of communication message format between policy server and policy client

Interaction between the policy server and the policy client carries out through a series of messages, so the design of each message format is very important for the system implementation, which includes message types and message format defined according to specific application requirements. This library workgroup-based policy system refers to the SPP protocol proposed by IPSec Working Group to design the communication message format between the policy server and the policy client. In this system, the policy client needs to send log on message, exit message, heartbeat message; the policy server needs to send log on response message, policy update message, client online notification message, client offline notification message, heartbeat message, and exit message. These messages ensure that the server automatically distributes group security policy to the group users logged on. And then these group users negotiate end-to-end IPSec SA parameters through the IKE service negotiation subsystem automatically.

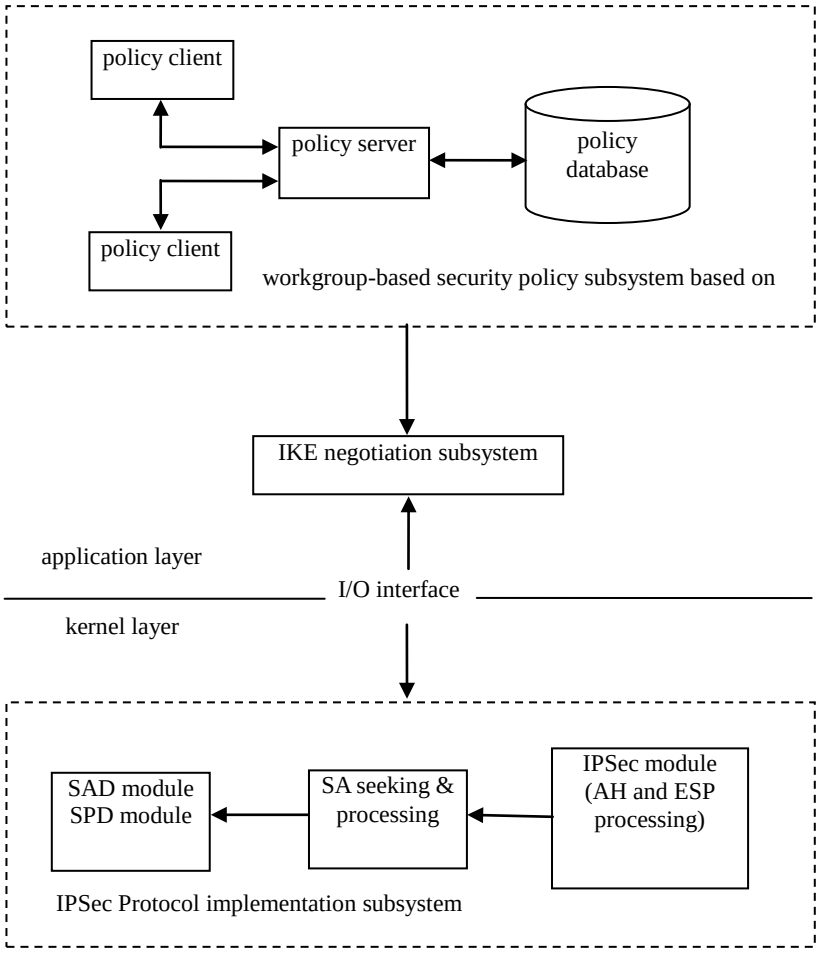

Figure 2 End-to-end security communication system architecture

3.3.3. System reliability and security

The communication message transmitted between the policy server and the policy client is based on UDP protocol. Because UDP does not provide end-to-end reliable data transmission service, so different sequence numbers are added to the header of each message and a timeout timer is started after the message is sent out. This mechanism can best ensure message transmission reliability at the application layer. The security policy system acts as a subsystem of the whole end-to-end communication system. So the subsystem's own security is also a key factor affecting the security of the entire end-to-end communication system. It is difficult to imagine that a security policy system to be able to trusted by customers if the system itself has potential security risks. Therefore the basic measure of encrypting communication messages to ensure the security of the policy system is required. And it should be able

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

to custom encryption algorithm based on customer confidentiality requirements. In the system implementation an encryption algorithm interface is provided to encrypt communication messages between the policy server and the policy client. The programmer can conveniently add different encryption algorithm through the interface, thereby increasing the flexibility of the system.

3.3.4. Policy translation from group security policy to IP-based policy

The most significant feature of this policy system is to put forward the concept of the library workgroup and group security policy. One library workgroup defines one or more group security policies distributed to all group users to protect end-to end communication security between them. But as we all know an IPSec tunnel is established between the end users on the basis of their IP addresses, so the group security policy needs to be translated into the IP-based policy which characterizes an IPSec tunnel between end users. The system takes the following approach: the policy client downloads an IP address list of all users logged on in the same library workgroup as well as the group security policy from the policy server. Then the policy client completes the task of translating the downloaded group security policy to the IP-based policy in local host. This processing strategy can not only reduce the burden of the policy server, but also decrease the amount of data transmitted between the policy server and the policy client. As stated above the policy server simply sends a list of IP addresses and the group security policy to the policy client.

3.3.5. Policy server and policy client exception detection mechanism

In network communication program, exception raised by the client or the server may usually leads to some errors, some of which the system can expect and handle while others of which may cause some serious problems beyond system expectation. For example, in the policy system if the client user exited abnormally, the policy server would not receive expected exit message from that client user so that the policy server would not detect the change in client status. At the same time the abnormal exit client cannot delete the previously established IPSec SA, and thus poses a security risk to the system. The way to solve this kind of problem is that both the policy server and the policy client send a message regularly to report its login status to each other, and such message is known as the "heartbeat" message. “Heartbeat” message sending interval depends on the application requirements. If the server (or client) does not receive the message after the time interval, then the client (or server) must go into an abnormal status. The exception detection mechanism can further ensure the policy system secure, stable and reliable.

4. CONCLUSIONS

This article proposes a convenient and efficient means for the implementation of IPSec by building a security policy system based on the library workgroup concept. This IPSec implementation in combination of group security policy system can be used as a solution for the problem of end-to-end communication protection. Currently, the development of all the modules of the group security policy system has been completed and the joint testing combined with the underlying IPSec and IKE programs has been carried out. The test results show that centralized configuration and correct distribution of the group security policy can be realized in the group security policy system.

Table 2 Wordnet3.0 Database Statistics Data

Word property / Statistics	Noum	Verb	Adjective	Adverb	Totals
Unique Strings	117798	11529	21479	4481	155287
Synsets	82115	13767	18156	3621	117659
Word—Sense Pairs	146312	25047	30002	5580	206941
Monosemous Words and Senses	101863	6277	16503	3748	128391
Polysemous Words	15935	5252	4976	733	26896
Polysemous Senses	44449	18770	14399	1832	79450

The next work is to consider expanding the concept of the library workgroup to multiple security domains. That means the group security policy system can cross gateways between different security domains so as to meet the requirements that users in the same library workgroup may come from WAN.

Whether the general ontology library system or professional domain ontology library system are widely valued and used online knowledge repository in natural language processing. They have been used in various fields of natural language processing, such as the elimination of syntactic ambiguity, semantic ambiguity to resolve, information retrieval and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

machine translation. Ontology library described above have their own advantages and irreplaceable, and also have their own stable user groups. The ontology library researchers or developers are trying to make them tend to perfect, and hope to provide users with more friendly interface and more fully function. Of course, the ontology libraries are less than satisfactory. To truly resolve these problems, has yet to develop a standardized tool, and it needs to have some characteristics, such as a certain openness, and to provide a unified concepts system and common knowledge base; a uniform markup language format for input and output, and this is the Web standard markup language, and support multilingual and use the Unicode character set, and wide application in the field of AI and knowledge representation, be recognized by the domain experts and IT specialists.

REFERENCES

[1] S. Kent, R. Atkinson. Security Architecture for Internet Protocol [EB/OL]. http://www.ietf.org/rfc/rfc2401.txt, November 1998.

[2] M. Blaze, A. Keromytis, M. Richardson, L. Sanchez. IP Security Policy (IPSP) Requirements [EB/OL]. http://www.ietf.org/rfc/rfc3586.txt, August 2003.

[3] M. Baltatu, A. Lioy, D. Mazzocchi. Security Policy System: Status and Perspective [J]. Proceedings of the IEEE International Conference on Networks, 2000:278-284

[4] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, A. Sastry. The COPS (Common Open Policy Service) Protocol [EB/OL]. http://www.ietf.org/rfc/ rfc2748.txt, January 2000.

[5] M Condell, C Lynn, J Zao. Security Policy Specification Language [M].2000-03

[6] L A Sanchez, M N Condell. Security Policy system[S].Internet draft, 1998-11

[7] L A Sanchez, M N Condell.Security Policy Protocol[S].Internet draft, 1999-07