POLICY-BASED MANAGEMENT ARCHITECTURE FOR INTERNET VPN USING DEN

백 승진, 박 종태
경북대학교 대학원 정보통신학과
sjbaek@ain.knu.ac.kr, park@ee.knu.ac.kr

Abstract

As the Internet-based virtual private network is being widely deployed, VPN management technology and standard management schema is needed. Many researches are done by Internet Engineering Task Force (IETF) IPSEC WG and other vendors. In this paper, we present the DEN information model for VPN service, and extend IPSecServices class by defining IPSecPolicyConsumer class. We present the management architecture for Internet VPN with the security policy management mechanism that is one of issues in VPN management using these models. As an example, SLA management process using IPSecPoilcyConsumer class is shown.

1. Introduction

Due to the recent explosive use of the Internet, Intranet and Extranet are widely being deployed in order to facilitate the communication and group working activities among business partners and customers. There is an increasing need to extend networks to specific exterior.

Virtual Private Network (VPN) is simply defined as the 'emulation of a private wide area network (WAN) facility using IP facilities' [1]. In IP-VPN, the VPN service is provided over the Internet by establishing a virtual communication link between end-points using various tunneling protocols such as L2TP and IPSec. As VPN service becomes widely popular, the need for efficient VPN service management technology becomes very important. In VPN service management, the policy-based management scheme is being employed.

There have been research efforts for VPN management including VPN management in ATM networks [2], and others [3]. There have also have been several research efforts on policy-based management including works on the managed object modeling, formalization of policy representation, and policy-based management architecture [4,5]. However, there have been few research works on IP-VPN management. Recently, IETF IPSEC WG proposes a few standards for policy-based IP-VPN security management. These include Internet Drafts on Security Policy Specification Language, Security Policy Protocol, Security Policy Data Model, and Security Policy System [6,7,8].

We have presented policy-based hybrid management architecture for IP-based VPN in our previous work [10]. In this paper, we have extended the work by using DEN technology. We define the information models for VPN service, management applications, and security policies. An LDAP version 3 directory is used as a policy repository.

This paper is organized as follows. Section 2 describes the related works, and in Section 3, we present the information modeling for VPN service using DEN technology. Section 4 describes policy-based VPN management architecture and policy verification processes. In section 5, we show an example of SLA management using the proposed models and architecture. Finally, we conclude in Section 6.

2. Related Works

IETF Policy Framework Working Group (PFWG) has proposed generic policy-based management frameworks and models [12]. PFWG has three main goals. First, to provide a framework for policy-based management. Second, to define an extensible information model and specific schemata compliant with that framework that can be used for general policy representation. Third, to extend the core information model and schema to address the needs of QoS traffic management.

The Distributed Management Task Force (DMTF) is the standards organization that develops DEN. Most of the work is done in the Networks Working Group of the DMTF. CIM is concerned about information modeling independent of the underlying implementation. This means that CIM can be implemented by a directory, by a relational or object databases, or by other means. DEN extends CIM, but also defines optimizations that enable the object-oriented features of CIM to be mapped into a directory implementation. Currently only IPSec protocol models are proposed in DMTF drafts [11]. But it is not enough to present VPN services.

IETF IP Security Protocol Working Group (IPSEC) develops mechanisms to protect client protocols of IP. A security protocol in the network layer is developed to provide cryptographic security services that flexibly support combinations of authentication, integrity, access control, and confidentiality [8]. IPSEC WG also makes efforts to standardize the policy-based VPN management scheme [14]. These include Internet Drafts on Security Policy Specification Language, Security Policy Protocol, Security Policy Data Model, and Security Policy System [6,7].

As we mentioned in our previous work, security policy system that is presented in the IETF draft has some limitations to introduce global policy concepts.

3. DEN Information Model for VPN Service

3.1 IPSecServices Class

DEN specification defines schema and an information model for representing network element and service information and relationships gathered from the network using existing protocols and other sources of network information. An access protocol is also included to store and retrieve information [11].

The primary purpose of DEN is to separate the specification and representation of network elements and services from implementation details. A secondary purpose is to provide an extensible framework to represent vendor-specific functionality and implementation mechanisms by vendor-specific subclasses.

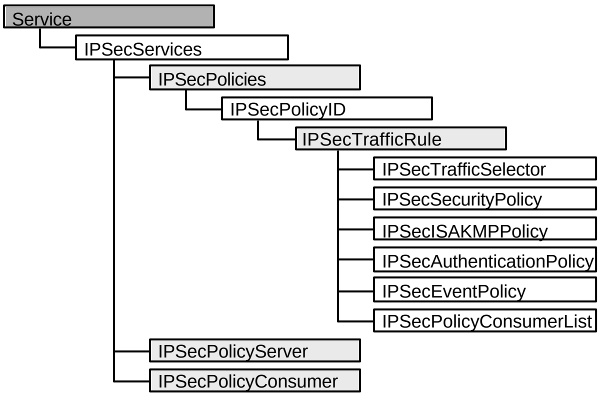

Figure 1. IPSecServices Class Hierarchy

Figure 1 shows the IPSecServices class hierarchy that is proposed by a DMTF draft [11]. IPSecPolicies class is composed of eight subclasses. Each subclass is related to IPSec policies and operation of IPSec-based VPN. This model is limited to IPSec protocol itself, and models for policy clients – namely consumer – are needed to present VPN services.

3.2 Definition of IPSecPolicyConsumer Class

DMTF draft describes the information model for IPSEC services. However, this is not enough to describe and to manage VPN services.

In this section, we define IPSecPolicyConsumer class for VPN service management, and extend IPSecServices class. Using class extension, VPN customer management can be achieved. In addition, customer's requests and policies used by customers can also be manageable.

Through class extension, we apply policy maintain level and user authority level that was described in our previous work [10]. As policies and service parameters can be described using DEN models, we can also describe and manage the factors that are related to customers – like SLAs.

We extend IPSecServices class by defining IPSecConsumer class as shown in Figure 2.

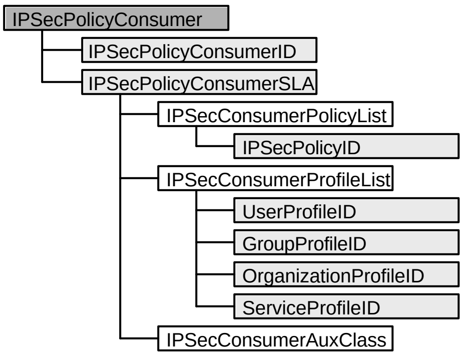

Figure 2. IPSecPolicyConsumer Class Hierachy

IPSecPoilcyConsumer class can be composed of following classes.

1) IPSecPolicyConsumer – a user of VPN services.
2) IPSecPolicyConsumerID – a set of attributes to describe a policy, such as an object id, user's name, description, version, revision, and reference its policies and profiles.
3) IPSecPoilcyConsumerSLA – a set of policies and profiles that are related to user's contract with service providers.

IPSecPolicyConsumerID described in Table 1 identifies a particular IPSecPolicyConsumer class and has a name and a description as attributes.

Class	IPSecPolicyConsumerID
Description	The root object which identifies a particular IPSec policy consumer, which will have references to component objects
Possible Superiors	Service::IPSecServices::IPSecPolicyConsumer
Must Attributes	Name, Description

Table 1. IPSecPolicyConsumerID

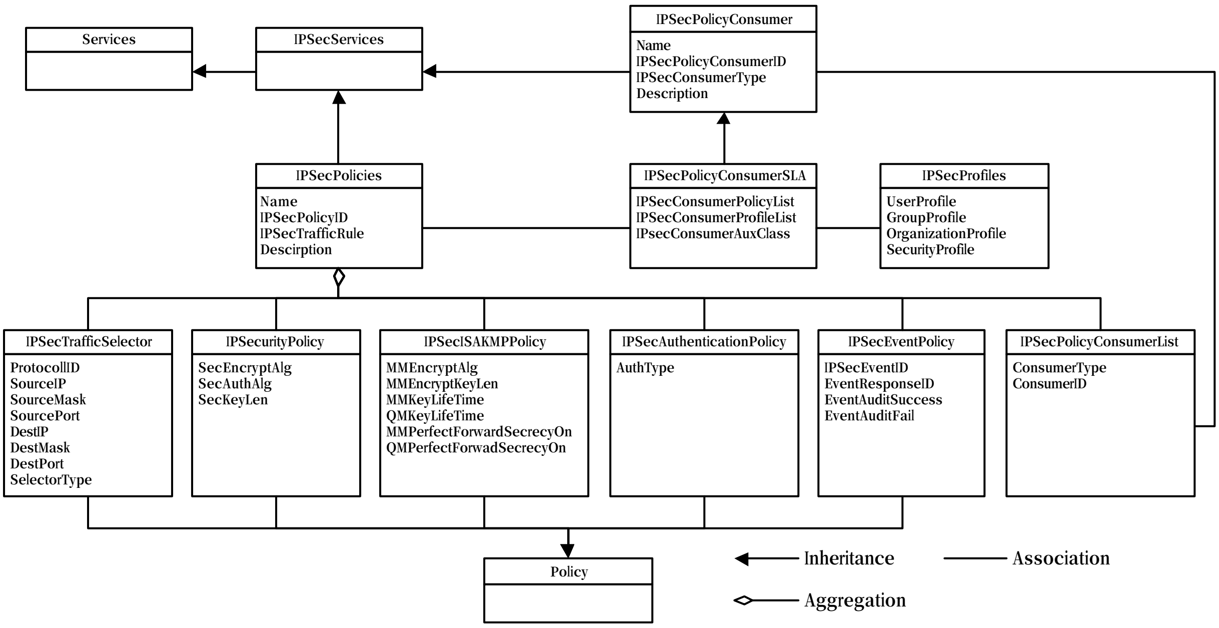

Figure 3. Class Diagram for VPN Services

IPSecPolicyConsumerSLA class in Table 2 represents the SLAs that are concluded between service providers and customers. Attributes of this class are a list of policy classes and a list of profile classes. IPSecConsumerAuxClass is a reserved class for later extension of other parameters.

Class	IPSecPolicyConsumerSLA
Description	Description for SLA between customers and providers.
Possible Superiors	IPSecPolicyConsumer
Must Attributes	IPSecConsumerPolicyList, IPSecConsumerProfileList, IPSecConsumerAuxClass

Table 2. IPSecPolicyConsumerSLA

Table 3 and Table 4 show the definitions of IPSec Consumer Policy List and IPSec Consumer Profile List. IPSec Consumer Policy List has one or more IPSec Policy ID. The policy of each ID affects on specific consumer class. IPSecConsumerPofileList has lists of user, group, organization, and service profile classes that are influenced on customer's environment.

Class	IPSecConsumerPolicyList
Description	Policy ID list that is involved with specific IPSecConsumerID
Possible Superiors	IPSecPolicyConsumerSLA
Must Attributes	IPSecPolicyID

Table 3. IPSecConsumerPolicyList

Class	IPSecConsumerProfileList
Description	Consumer's Profile
Possible Superiors	IPSecConsumerSLA
Must Attributes	UserProfileID, GroupProfileID, OrganizationProfileID, ServiceProfileID

Table 4. IPSecConsumerProfileList

Figure 3 shows the class diagram for VPN services based on extended classes. Figure 3 presents the related classes and their associations, inheritances, and aggregations.

4. Policy-based VPN Management Architecture

Policies describe management activities ranging from lower-level management operations to higher-level objectives that are determined by economical or social requirements. A policy determines the management objectives, the roles, and the responsibilities between a subject set containing managers and a target set containing managed objects. The manager applications can be made responsible for the enforcement of policies, i.e. they have to interpret policies and to align their behavior with the policies.

4.1 Design of Security Policy System

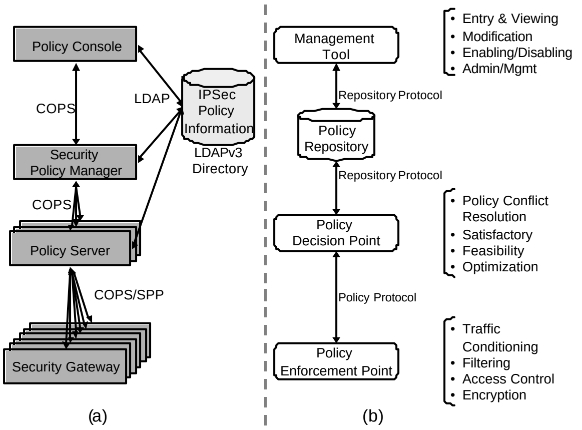

Figure 4. System Overview

We show a security policy system in order to eliminate the limitations imposed by the existing security policy system [7] submitted to IETF IPSEC WG using IPSecServices and IPSecPolicyConsumer classes.

Figure 4 (a) shows the functional modules of proposed system, which are compared with generic policy-based management functions that are shown in Figure 4 (b). The proposed security policy system plays a role of generic policy system. It distributes global policies, which are set up by VPN administrator, and verifies the consistency of the policies that are created or modified by local administrators. Figure 4 shows the overall structure of proposed security policy system, its components, and operations. Each component shown in Figure 4 has the functions as described below.

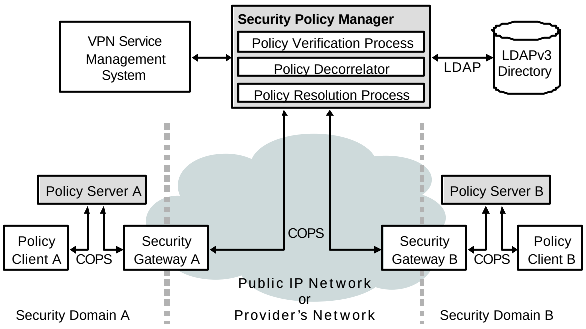

Figure 5. Interworking between Policy Server and Security Policy Manager

✍✍ Security Policy Manager (SPM)

In this system, Security Policy Manager (SPM) plays a role of policy decision point (PDP). SPM transfers not only policy to Security Policy Server (PS), but also response for policy query that PS has asked. It has global SPD to retain policy information of the entire network. The existing PSs communicate information with SPM, which does with the individual server by means of COPS, in order to exchange policy information. In other words, from the Policy Server's point of view, it only differs communication object but any other change. In addition to this, it only needs to retain location information of Security Policy Manager, instead of having location information of other Security Gateway.

SPM performs verification, decorrelation, and policy resolution process about a newly created and/or modified policy and stores the results at LDAP directory. It checks whether the local policy is consistently enforced through verification process. Policy decorrelation and policy resolution process is performed to add in the previous policy as well. Algorithms and procedures of decorrelation and resolution process are described in [16]. SPM can interoperate with VPN service management system for automatic provisioning and management of VPN service.

✍✍ Security Policy Server (PS)

The security policy server plays a role of enforcing policies into the security gateways. Policy servers exchange policy information with policy clients using COPS. In the architecture of [7], PS communicates with other PSs to check the authority for the specific host. However, in our system, servers interacts with not other PSs, but SPM. Policies that are made by local administrator must be verified by SPM through the policy verification process.

✍✍ Directory Services & LDAP

A directory is a special purpose database that contains information about the various resources available on a network. A directory service is quite different from a general DBMS in that directory information is attribute-based more descriptive in nature. These attributes give specific information about various objects to the clients of the directory service.

The access protocol for DEN information is LDAP (Lightweight Directory Access Protocol) version 3. In the proposed system, a directory stores the policies in the form of DEN information. SPM can access the information using LDAP.

✍✍ Policy Verification Process

SPM inspects the requested policy through policy verification process. To achieve this function, this process may include user authentication and verification of the authority on the request

In DEN models, the IPSecPolicyConsumer class represents the owner of it. If a new policy is created, IPSecPolicyConsumerList should have the value of all the affected users. From the view of service provider, he or she must restrict the customers within the scope of the contract or SLA. On the other hand, customers may change their services within the scope of the contract. In this case, the various policy levels and user classes are needed.

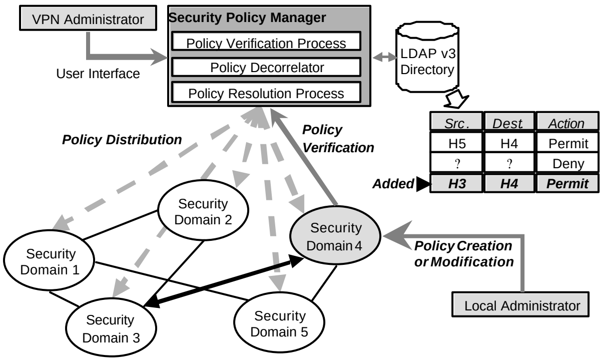

Figure 6. Policy Verification Process

✍✍ Policy Verification Algorithm

Policy verification process verifies the authority of users as follows.

① Authenticate user identity.

② Get the authorized domain list in IPSecConsumer class

③ Get the customer's authority level from Policy Authority Table

④ Break up the policy C into the smaller sets $C_1 ? C_2 ? \square \; ? C_k$, as described below, such that there is no loss of policy information.

$C \; ? \; C_1 ? C_2 ? \square \; ? C_k$

C : Policy that is requested by users

C_j : The *j*th policy in C

⑤ Compare every C_j with policies in the directory.

⑥ Send COPS DEC message with an error object to the user when a user is found to have no authority. This means customer's authority level is lower than that of the existing policy.

⑦ Send COPS DEC message to the user when a user has the authority. COPS DEC message includes the associated client handle and one or more decision objects. The new policy is added to SPD through the decorrelation and resolution process.

Procedures and algorithms for resolution and decorrelation are described in [7].

5. Application of Extended Model to SLA Management

We describe the operations of security policy system in the case of SLA management. SPM distributes the policies based on SLAs to each local PS in the proposed architecture. The VPN administrator can make and modify the policies and SLAs. Policies that are made by the VPN administrator are stored in the policy directory through the policy decorrelation process module in SPM. Policies stored in the directory are distributed to the local servers using policy protocols – COPS, SPP, and so on. In our system, a VPN administrator can enforce the global policies based on SLAs to local policy servers automatically as follows.

① VPN service providers and customers make a new SLA and related security policies.

② The policies are delivered to SPM by either manual manner or using visualized tools.

③ The received policies are decorrelated and merged with existing policies.

④ SPM makes new instances of IPSecPolicies class and its subclasses to store the new policies.

⑤ SPM adds IPSecPolicyID to IPSec Consumer Policy List class.

⑥ The policy class is stored in directory.

⑦ SPM sends COPS DEC messages to related policy servers.

⑧ Finally, the new policies are enforced at policy servers and security gateways.

6. Conclusion

In this paper, we have proposed a policy-based VPN management architecture. We also have extended IPSec Policy Service class by defining IPSec Policy Consumer class. Using extended DEN information model for VPN services, security policy manager enforces security policies, and manages security policies with several functions, which are necessary for the verification, decorrelation, and resolution. We have extended the policy verification process and algorithms using DEN model. For an illustrating example, the SLA management process has been shown that is based on DEN information model. The system simplifies the service provisioning procedure and policy negotiation procedure, and achieves more efficient management performance. In the future, we will evaluate the performance and scalability of the proposed system.

[Acknowledgements]

This work is supported in part by the Ministry of Information & Communication of Korea ("Support Project of University foundation research<' 99>" supervised by IITA).

[References]

[1] Bryan Gleeson, Arthur Lin, Juha Heinanen, Grenville Armitage, and Andrew Malis, "A framework for IP based Virtual Private Networks," Internet Draft, 1999.

[2] J. T. Park, J. H. Lee, J. W. Hong, Y. M. Kim, and S. M. Kim, "A VPN Management Architecture for Supporting CNM Services in ATM Networks," Proceeding of the IEEE/IFIP International Symposium on Integrated Network Management, pp.44-57, May 1997.

[3] M. C. Chan, A. A. Lazer, and R. Stadler, "Customer Management and Control of Broadband VPN

Services," Proceedings of the Fifth IFIP/IEEE International Symposium on Integrated Network Management, May 1997.

[4] B. Alpers and H. Plansky, "Concepts and Application of Policy-Based Management," Proceeding of the IEEE/IFIP International Symposium on Integrated Network Management, pp. 57-68, 1995.

[5] Stephen Howard, Hanan Lutifyya, Michael Katchaban, and Michael Baurer, "Supporting Dynamic Policy Change Using CORBA System Management Facilities," Proceeding of the 5th IFIP/IEEE International Symposium on Integrated Network Management, May 1997.

[6] M. Condell, C. Lynn, and J. Zao, "Security Policy Specification Language," Internet Draft, July 1999.

[7] L. A. Sanchez and M. N. Condell, "Security Policy System," Internet Draft, November 1998.

[8] S. Kent and R. Atkinson, "Security Architecture for the Internet Protocol," RFC 2401, November 1998.

[9] J. W. Baek, T. J. Ha, J. T. Park, J. W. Hong, and S. B. Kim, "ATM Customer Network Management Using WWW and CORBA Technologies," Proceeding of the IEEE/IFIP Network Operations and Management Symposium, New Orleans, Louisiana, pp.120-129, February 1998.

[10] Seung-Jin Baek, Moon-Sang Jeong, Jong-Tae Park, and Tai-Myung Chung, "Policy-based Hybrid Management Architecture for IP-based VPN," Proceeding of the IEEE/IFIP Network Operations and Management Symposium, April 2000.

[11] DMTF, "Network Services – Internet Protocol Security," DMTF Draft, February 1998.

[12] M. Stevens, W. Weiss, H. Mahon, B. Moore, J. Strassner, G. Waters, A. Westerinen, and J. Wheeler, "Policy Framework," Internet Draft, September 1999.

[13] Francis Reichmeyer, Kwok Ho Chan, David Durham, Raj Yavatkar, Silvano Gai, Keith McCloghrie, Shai Herzog, and Andrew Smith, "COPS Usage for Policy Provisioning," Internet Draft, February 1999.

[14] Partha Bhattacharya, Rob Adams, William Dixon, Roy Pereira, and Raju Rajan, "An LDAP Schema for Configuration and Administration of IPSec based Virtual Private Networks (VPNs)," Internet Draft, October 1998.