A Policy-based Network Management System for IP VPN

Xin Guo, Kun Yang, Alex Galis  
University College London,  
Department of Electronic and Electrical Engineering, Torrington Place, London  
WC1E 7JE UK  
{xguo, kyang, agalis}@ee.ucl.ac.uk

Xiaochun Cheng  
1) University of Reading, Dept. of Computer Science, Reading, RG6 6AY, UK  
2) Beijing Normal University, China  
Northeast Normal University, China  
x.cheng@reading.ac.uk

Bo Yang, Dayou Liu  
Jilin University,  
School of Computer Science, 10 Qianwei Road, Changchun, Jilin,  
130012. P. R. China  
{yangbo, dyliu}@mail.jlu.edu.cn

Abstract: Even though IP VPN has practically proven itself to be a cost-effective solution, the lack of centralized network management capabilities of current IP VPN deployment makes the management of growing VPN networks an extremely tedious procedure. This paper proposes to use policy-based network management method to address this challenge. Firstly, a policy-based IP VPN management architecture is presented, mainly explaining the operational components concerning the IPsec. Then a detailed discussion with respect to policy definition language and IP VPN policy information model is given. Finally, a case study for inter-domain IP VPN configuration exemplifies the design and implementation of this management system based on the testbed developed in the Networks & Services Group of University College London (UCL).

Keywords: IP Virtual Private Network (VPN), IPsec (IP Security), Policy-based Network Management (PBNM)

I. INTRODUCTION AND BACKGROUND

Traditionally, organizations interconnected their distributed sites by a private network that was facilitated through a set of links comprising of dedicated circuits (T1, T3 etc.). This approach provided predictable performance and security to the user. However, this solution is expensive and not very flexible. The Virtual Private Network (VPN) enables an organization to interconnect its distributed sites over a public network. From a user’s viewpoint, a VPN ideally looks and behaves like a traditional private network. Several issues need to be addressed in order to fulfill IP VPN, of which security is the most important one. A good candidate to solve security problems that arises during provisioning of a VPN service via public networks is IPsec (Internet Protocol Security) [1]. It is applied on the network layer and provides a set of security services that cover data confidentiality, integrity, authentication, key management, and tunneling.

But even though VPNs have proved to be cost-effective solutions, the lack of centralized network management capabilities of current IP VPN deployment makes the management of growing networks time-consuming and error-prone. A flexible and automated management of IP VPN is getting increasingly imperative. The emerging policy-based network management paradigm claims to be a solution to this requirement.

Policy-based network management (PBNM) has been the subject of extensive research over the last decade [2]. Policies are seen as a way to guide the behavior of a network or distributed system through high-level declarative directives. In comparison with previous traditional network management approaches, such as TMN or TINA-C, PBNM offers a more flexible, customizable management solution that allows controlled elements to be configured or scheduled on the fly. The Internet Engineering Task Force (IETF) Policy Framework Group [3] has been investigating policies as a means for managing IP-based networks.

The goal of IP VPN management is to provide a flexible way for network administrator to manage large networks as a single entity rather than hundreds or thousands of discrete elements. The administrator needs to be protected from the differences between the different technologies and network topology that are used by network elements and networks to provide this capability. The IP VPN Policy Information Model [4] defined by IETF mainly focuses on the network level specification which helps translate service level specifications to device level configuration for IP VPN services; whereas less concern is given to the management of IP VPN in a higher level that can be beneficial to the VPN providers. This paper aims to develop a PBNM system for higher level management of IP VPN.

This paper first discusses a policy-based IP VPN management architecture with emphasis on the functional components of IPsec; then a detailed explanation with respect to policy definition language and IP VPN policy information model is presented. Finally, before the conclusions, a case study for inter-domain IP VPN configuration is demonstrated, aiming to exemplify the design and implementation of this management system.

II. A POLICY-BASED IP VPN MANAGEMENT ARCHITECTURE

A. Architecture Overview

A policy-based IP VPN management system architecture and its main components are depicted in Figure 1, which is organized based on the PBNM concept.
Linux

Internet which is a shared public network with open transmission protocols, VPNs must include measures for security) protocols. Since IP VPN is built up via the packet encapsulation (tunneling), encryption and authentication so as to avoid the sensitive data from being tampered by any unauthorized third parties during data transit. Three protocols are used: AH (Authentication Header) provides a packet-level authentication service; ESP (Encapsulating Security Payload) provides encryption plus authentication; and finally, IKE (Internet Key Exchange) negotiates connection parameters, including keys, for the other two. KLIPS (kernel IPsec) from FreeS/WAN has implemented AH, ESP, and packet handling within the kernel [6]. Since KLIPS is working beyond the management plane and based on the result of IKE, more discussion is given to IKE issues which are closely related to the policies delivered by administrator via policy management tool.

B. SLA Management: SLA Registration & SLA Enforcement

Starting from the SLA (Service Level Agreement) management part on the left of PDP block, the SLA Registration (SLA-R) component includes processes for customer registration. Customer registration concerns the service level agreement, containing prices, terms, conditions, and the technical parameters that are known as Service Level Specification (SLS). SLA-R helps set up the initial policies guiding VPN configuration in the way that it instantiates values requirement by IKE and SAs. SLA Enforcement (SLA-E) is the functional block that fulfils the enforcement of SLAs resulted from SLA-R, and it involves processes of triggering IKE management component which, as a result, sets up IPsec connections after the finish of negotiation. SLA-E can be considered as part of policy decision functionality for initiating the lifecycle of policy enforcement. It performs dynamic policy decision making based on the information retrieved from Monitoring component after receiving input from the SLA-R. Finally SLA-E delegates the necessary policies to the Key Management component.

C. Key Management Component

Encryption usually is the starting point of any VPN solution. These encryption algorithms are well known and widely exist in lots of cryptographic libraries. Using symmetrical keys in smaller VPNs does not necessarily require complex mechanism for key management. However, larger networks have to exploit asymmetrical keys system to avoid the manual distribution of symmetrical keys, therefore require the needs for key management. These features need to be taken into consideration for key management component: key generation, key length, and key exchange mechanism.

D. IKE Management

IKE protocol was developed to manage these key exchanges. Using IPSec with the IKE, a system can set up security associations (SAs) that include information on the algorithms for authenticating and encrypting data, the
lifetime of the keys employed, the key lengths, etc; and these information are either extracted from SLA or guided by policies stored in the policy repository. Each pair of communicating computers will use a specific set of SAs to set up a VPN tunnel. IKE negotiations have two phases. Firstly, the two gateways negotiate and set up a two-way ISAKMP SA. One such SA between a pair of gateways can handle negotiations for multiple tunnels. Then, using the ISAKMP SA set up in phase one, the gateways negotiate IPsec SAs as required. After both IKE phases are complete, IPsec SAs carry the encrypted data.

The core of the IKE management is an IKE daemon that sits on the node to which SAs need to be negotiated. IKE daemon is distributed on each node that is to be an endpoint of an IKE-negotiated SA. IKE protocol sets up IPsec connections after negotiating appropriate parameters. This is done by exchanging packets on UDP port 500 between two gateways.

E. Other Components

SA Management: Given any significant number of hosts communicating over a VPN, the number of SAs that need to be negotiated for a VPN session can be enormous. While the negotiation of cryptographic and other security parameters for IPsec SAs is supported by key management protocols, the IPsec key management layer doesn’t provide a scheme for managing, negotiating, and enforcing the security policies under which SAs operate. The PBNM system presented in this paper provides a potential solution for this.

The ability of cohesively monitoring all VPN devices is vitally important. It is essential to ensure that SLAs are being satisfied by determining the level of performance and know what in the network is not working properly if there are. Necessary information such as how long a device has been down or where exactly the SLA failed can be captured by this monitoring component. VPN devices can be monitored for general performance as well as for more detailed parameters useful in determining more specifically what caused problems. The monitoring component drawn in PDP box is actually a monitoring client for enquiring status of VPN devices or links. The real monitoring daemons are located next to the monitored elements and are implemented using different technologies depending on the features of monitored elements.

The presence of Domain Management is to distinguish inter-domain policies from intra-domain policies in order to make the policy management more efficient.

III. POLICY LANGUAGE AND INFORMATION MODEL

Based on the policy-based IP VPN system architecture presented in the previous section, this section details the design and implementation of this PBNM architecture in terms of two critical PBNM concerns, i.e., policy definition language and policy information model. PBNM system explored in this paper is based on policy framework proposed by IETF [3].

F. Policy Definition Language

A high level policy definition language has been designed and implemented to provide the administrator with the ability of adding and changing policies in the policy repository. Policy takes the following rule-based format:

\[ \text{[PolicyID]} \text{ IF } \{ \text{condition(s)} \} \text{ THEN } \{ \text{action(s)} \} \]

It means \text{action(s)} is taken if the \text{condition(s)} is/are true. Policy condition can be in both disjunctive normal form (DNF, an ORed set of AND conditions) or conjunctive normal form (CNF, and ANDed set of OR conditions), as recommended by IETF Policy workgroup. PolicyID field defines the name of the policy rule and is also related to the storage of this policy in policy repository.

An example of policy is given below, which forces the SA to specify which packets are to be discarded.

\[
\text{IF } \{ \text{sourceHost} == \text{Camden} \} \text{ and } \{ \text{EncryptionAlgorithm} == \text{3DES} \} \text{ THEN } \text{IPsecDiscard}
\]

This rule-based policy is further represented by XML (extensible Markup Language) due to XML’s built-in syntax check and its portability across the heterogeneous platforms. The schema of the XML file is fully in line with the schema of LDAP-based policy repository.

G. Policy Information Model

An object oriented information model has been designed to represent the IP VPN management policies, based on the IETF PCIM (Policy Core Information Model) [7]. The major objective of such information models is to bridge the gap between the human policy administrator who enters the policies and the actual enforcement commands executed at the network elements. IETF has described an IPsec Configuration Policy Model [4], representing IPsec policies that result in configuring network elements to enforce the policies. Our information model extends the IETF IPsec policy model by adding more functionalities sitting at a higher level (network management level).

Figure 2 depicts a part of the inheritance hierarchy of our information model representing the IP VPN policies. It also indicates its relationships to IETF PCIM. Some of the actions are not directly modeled due to the space limitation. Please note that apart from the PolicyAction and PolicyCondition as described above, the IPsec actions such as IPsecBypassAction and IPsecDiscardAction are also reflected in this policy information model.
Security policies define acceptable access privileges, which may depend upon combinations of factors including job titles, special projects, need-to-know, and level of trust. In addition, policies should be granular enough to allow differentiation by organization, server, group, and even user levels.

IV. Case Study: Inter-domain IP VPN

Based on the IP VPN management infrastructure and information model discussed above, this section presents a case study to evaluate this architecture, i.e., inter-domain IP VPN provisioning guided by policies. Inter-domain communication is also a challenging research field in network management. This paper manages to address this issue, as a case study, from the security’s perspective. This scenario was implemented in the test-bed developed in the Network & Services Group of University College London.

V. Conclusions and Future Work

This paper presents a policy-based IP VPN management system. The work described in this paper complements the IETF IPsec Configuration Policy Model that focuses on the control plane of IPsec configuration in the sense that it emphasizes on the network management level of IP VPN. Based on the discussion of IPsec functional components, the appropriate policy definition language has been discussed and an IP VPN policy information model was described. An inter-domain IP VPN provisioning finally demonstrated the implementation status and its flexibility and automation in managing IP VPNs.

Defining a full range of policies regarding IP VPN management and the study of how they can coexist together towards a practical application are the future work. Policy conflict check and resolution mechanisms will also require more work as the number of policies dramatically increases.

REFERENCES