A Design of Scalable SNMP Agent for Managing Heterogeneous Security Systems

D. Y. Lee, D. S. Kim ,K. H. Pang, H. S. Kim and T. M. Chung
Real-Time Systems Laboratory
Dept. of Electrical and Computer Engineering, Sungkyunkwan University 300 Chun-chun-dong, Changan-Gu, Suwon City, Kyounggi-Do
South Korea
(dylee, dskim, khpang)@rtlab.skku.ac.kr, *hskim@securesoft.co.kr, and* tmchung@ece.skku.ac.kr

Abstract

This paper presents the web based integrated security management system (WISMS) which have been developed to monitor and control heterogeneous security systems and detailed design of firewall agents. The agents perform the control requests from security manager, maintain firewall MIB, and reports monitored status of firewall

Among the issues raised by the expansion of networks in Internet environments, security management to protect networks from intrusions and attacks have been given much attention. Such attacks are computer viruses, hackings to destroy information, and denial of service attacks. To protect networks from those attacks, many vendors have developed various security systems such as firewalls and intrusion detection systems. However, individually managing those systems requires too much work and high cost. Thus, developing integrated security management for security products has become more important even though it is not an easy task because of the system property such as scalability, heterogeneity, and efficiency issues. Therefore, we have been developed a web-based integrated security management system for firewalls called WISMS, that has an integrated management facility to manage various firewalls such as SecureShield, TIS-FWTK, and ipfwadm of Linux kernel packet filer. The proposed WISMS architecture is illustrated in Figure 1.

WISMS is designed based on master-client paradigm that consists of clients, integration engine, and agents. Then, we present firewall agents which is one of many types of security systems such as IDS, Authentication Server, and others. Firewall agents manage various types of firewalls based on master-agent paradigm. The design of agent focuses on the scalability to newly introduces or expanded firewall structure so that minimal changes may be needed to manage another firewall. An agent initiates with SNMP security MIB, monitors the status of a firewall, and processes control requests from integration engine. In order to make the agent scalable, we propose a two-fold architecture of firewall agents - modularized security agent for firewall(MSAF)

MSAF consist of two folds - distinct module to focus on its own control facility, and common module identical to among agents. They are application dependent module(ADM) and integrated common module (ICM). The major functionality of the ICM is to provide the same control interface to WISMS engine regardless of the types of firewall application that MSAF manages. ADM has the function of direct control over individual firewall application.

0-7803-5864-3

It executes application-dependant operations. The managed firewalls form different vendors have specific ways of controlling their security products. Thus, ADM is implemented differently in terms of the methods for enforcing policies in each application. With separated structure of MSAF, an agent may offer the same interface to the WISMS engine with no consideration of the firewall type. In this way, transparency is provided to users.

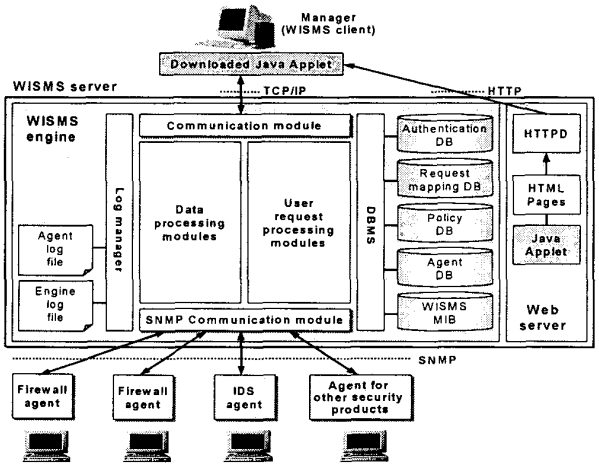

Figure 1 : Proposed WISMS Architecture

For the interface between agents and engine, the standard network management protocol, SNMP is used and the transmission of control requests, monitored data, and SNMP security MIB data are secured via tunneled communication between agents and engine. Engine-agent interface (EAI) supports data encryption standard(DES) which is one of the cryptographic algorithms recommended in SNMP v3.

We defined the MIB objects of WISMS are temporarily defined under enterprise(4) node of OID tree currently. WISMS is originally the part of the web-based integrated security management system. Therefore, the current MIB for firewall application management, the firewallMIB(0), is defined under the OID named WISMS(1999). We will plan to define additional MIB for WISMS that will manage various network security applications over widely spread network. For example, nidsMIB is reserved for managing network-based intrusion detection system (NIDS).

The firewallMIB(0) is divided into two major parts; Common MIB and Application dependent MIB. The Common MIB named accessControlAppMIB(0) is common to all MSAF and defined under the node firewallMIB(0). It generalizes the common functions and information from heterogeneous firewall applications by testing firewall systems in our test environment that is composed of independent small LANs. And, the Common MIB is consists of four parts – Application information MIB, Policy table, Session table, and Traps. The OIDs of application dependent MIB are also defined under the firewallMIB(0), and they are named after the name of each firewall applications. They are used for managing functions and information dependent on each application. For example, the secureshieldMIB includes MIB objects for controlling virtual private network (VPN) policy that is uncommon to other firewall applications, exclusively.

Finally we will develop prototype WISMS and resolve the problems derived from the verification of implemented system. And also, we will extend WISMS which supporting security systems such as IDS, VirusWall, and others.