Enhanced Network Security Management using Role

JONG-GOOK KO, JEONG-NYEO KIM, SUNG-WON SOHN
Electronics and Telecommunications Research Institute(ETRI)
161 Kajung-dong, Yusung-gu, Taejon 305-350
Korea
{jgko, jnkim, swsohn}@etri.re.kr

Abstract: - Network security management is attracting a special attention in recent times. There are many kinds of security technologies and tools to protect IT systems and organizations. Each security tool is important aspects of security but, the effective management of the tools is most critical. In this paper, we present two kinds of framework for network security management. At first, This paper propose network management model using role-based access control (RBAC) that is used to control access to network node such as router, firewall and switch and so on. Secondly, it also introduce policy based network management and propose Role and Policy-based Network Security Management (RPNSM) model which enhance the policy-based network management by using role.

Key-Words: - Policy based Network Management, RBAC, Role.

1 Introduction

Today's networks are complex connections of resources that often are difficult to manage. Network managers are still struggling with the configuration of individual devices such as router, firewall and switch and so on. In an effort to mitigate the growing complexity of network management, the networking industry is beginning to recognize the need to develop network management technologies. The emerging policy-based network management paradigm is a direct result of this need. Policy based network management [1,2,3] is an approach that manages network components using high-level policies. There are very important application of policy-based network management One is for QoS, other is for Security. In this paper, we are focusing on security. Policy-based networking can be helpful to manage network, since it makes it easier to relate the configuration of devices to management's security policy and promotes consistency of policies to all affected devices from a central store. For example, suppose that the security access policy for a company changes so that it now allows FTP services for selected hosts. Management by policy will allow the administrator to enter a policy that grants access to FTP services for the appropriate hosts. And the policy is applied to each affected firewalls automatically. On the other hand, without policy-based, the administrator should individually create ACL entries on all affected firewalls or IP-filtering devices to grant access to the FTP services for each selected hosts. The difficulty comes whenever dealing with a multitude of changes for many servers, firewalls, and router. This is not be a serious problem for a small company, but as size and complexity of the company grows, managing security without a policy-based system becomes obstacle.

In this paper, we describe network management using role based access control (RBAC). Role based access control is used to control an access to network node. One of attacks of routers is getting the super-user privilege. For example, if the super user privilege of router is hacked by SNMP vulnerability [4], then the managed sub networks are exposed to threat by compromising the router's filtering rule.

The rest of this paper is organized as follows. A brief description on role-based access control and policy-based network management is contained in section 2. Section 3 describes how the RBAC is employed to control access to network node for protecting the network node from unauthorized action. Section 4 describes policy based network security management using roles. Conclusions are discussed in section 5.

2 Background Information

Role Based Access Control (RBAC)[5,6,7] is an alternative to traditional discretionary (DAC) and mandatory access control (MAC) policies that is attracting increasing attention, particularly for commercial applications. The principle motivation behind RBAC is the desire to specify and enforce enterprise-specific security policies in a way that maps naturally to an organization's structure. RBAC is described in terms of individual users associated with

roles as well as roles associated with privilege. As such, a role is a means for naming many-to-many relationships among individual users and unique privilege. A user in this model is a human being. A role is a job function within the organization with some associated semantics regarding the authority and responsibility conferred on the user authorized for the role. Figure 1 describes the relationship between users, roles and privilege.

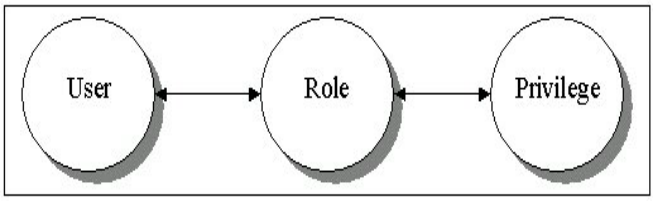

Fig.1. Basic Role based Access Control Model

Policy based networking offers a network manager the ability to manage the network in a dynamic fashion rather than force a network manager to manage the network by dealing with each device individually. In essence, policy-based networking allows network managers to express business goals as a set of rules or policies, which are then enforced throughout the network. This architecture makes it possible to apply rules either enterprise-wide or within domains, such as specific user groups or geographic areas. Policy-based network management systems consist of the following components: policy console, policy management tool, policy repository, policy decision points, and policy enforcement points. Policy console serves as the interface between the human network manager and the rest of policy management systems. The function of the policy management tool is driven by the policy console. Policy management tool translates the policies created at the console and handles communications with the policy repository on behalf of the console. Policy management tool also has the responsibility of notifying policy decision point (PDP)s of changes in policies. The primary purpose of policy repository is to store the policy rules that are created for the policy based management system. Policy decision point (PDP) makes policy decisions and transmits policies to the policy enforcement points. The PDP therefore maintain a list of the policy enforcement points that it is responsible for. Policy enforcement point (PEP) is the point where the policy decisions are actually enforced. Many of the protocols already used for PDP-PEP communications, such as CLI, SNMP, HTTP, and CORBA that can be used to distribute policy-based device configurations to PEPs. Another protocol, Common Open Policy Service (COPS) protocol, has also proposed for exchanging information between PDP and PEP. Figure 2 depicts configuration of policy based network management system.

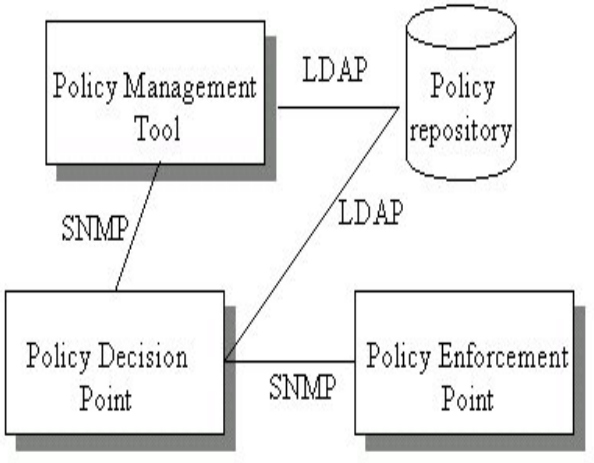

Fig.2. Policy based Network Management Model

3 Access Control to Network Node using Role-Based Access Control(RBAC)

Using conventional mechanisms(for example, SNMP and CLI) centralized network management applications implement network policy by pushing configuration information into network devices individually. Figure 3 depicts the simple network management system. If the agent in network device receive configuration command from network manager through SNMP then, it process updating the configuration file (e.g. : router's ACL) for security management. Suppose that unauthorized user have attacked the network device using SNMP vulnerability. Then the unauthorized user can compromise everything of network device. The Computer Response Team Coordination Center (CERT/CC) issued an advisory to all network administrators of a flow (e.g. : buffer overflow and format string errors) in the Simple Network Management Protocol (SNMP), the protocol used to remotely administer routers, switches and network management systems.

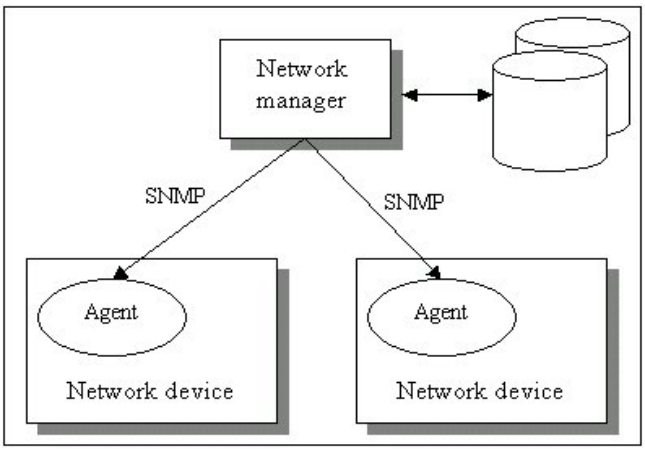

Fig. 1. Simple Network Management Model

In this paper, we propose network security management framework using RBAC that control access to network device. By using RBAC, it protects the resource of network device from unauthorized access and also assigns users proper privilege for their responsibility and role. Figure 4 depicts network security management system using role-based access control.

Network security management using RBAC is consists of following components.

- Network Manager: user or client that manage to make network secure.
- Network device: the device where the security commands or policies are enforced.
- Role Certificate Server: certificate server where authenticate and assign role
- Access Control Server: server where decision are made with access information
- RBAC admin: setup relation between role and privilege

Network manager at first, get a proper role after being authenticated from role attribute server and send management police to the affected network device with assigned role. Before network device processes management task (e.g., configuration of router's ACL), it send access decision request to access control server. Access control server makes decision with access information such as the relation of role and privilege. The example of role and privilege are like following:

- Role: operator role, manager role, subnet manager role and so on.
- Privilege: "modify filtering rules", "change routing table" and so on.

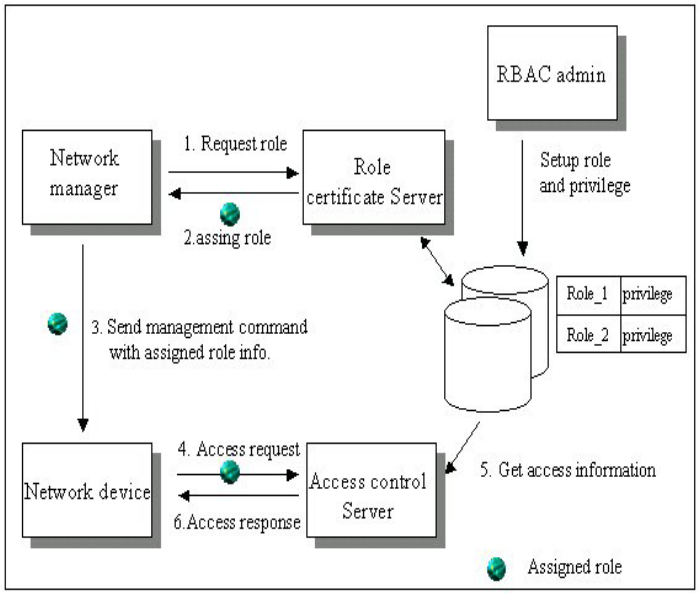

Fig. 2. Network Security Management using RBAC

4. Role & Policy based Network Security Management (RPNSM)

In section 3, we have proposed simple network security management using roles that is just used to control access. In this section, we present other kinds of role additionally. In other words, we present policy based network management model using role. Roles make enhance the policy-based management by supporting efficient management function.

4.1 Existing Policy-based Network Security Management Model

As described in section 1 and section2, Policy-based networking can be helpful to manage network, since it makes it easier to relate the configuration of devices to management's security policy. Instead of actively iterating through a list of devices and configuring them one by one, policy-based network management configure network device automatically using policies. Policy-based network management use policy rules to define the desired behavior of a wide range of devices running in a given network. When the network manager has changed policy rules in policy repository, policy decision point (PDP) or policy server should retrieve the policy of affected network device from policy repository and it apply the changed policy rules to network device automatically. In other words, the relation of between policy rules and network device

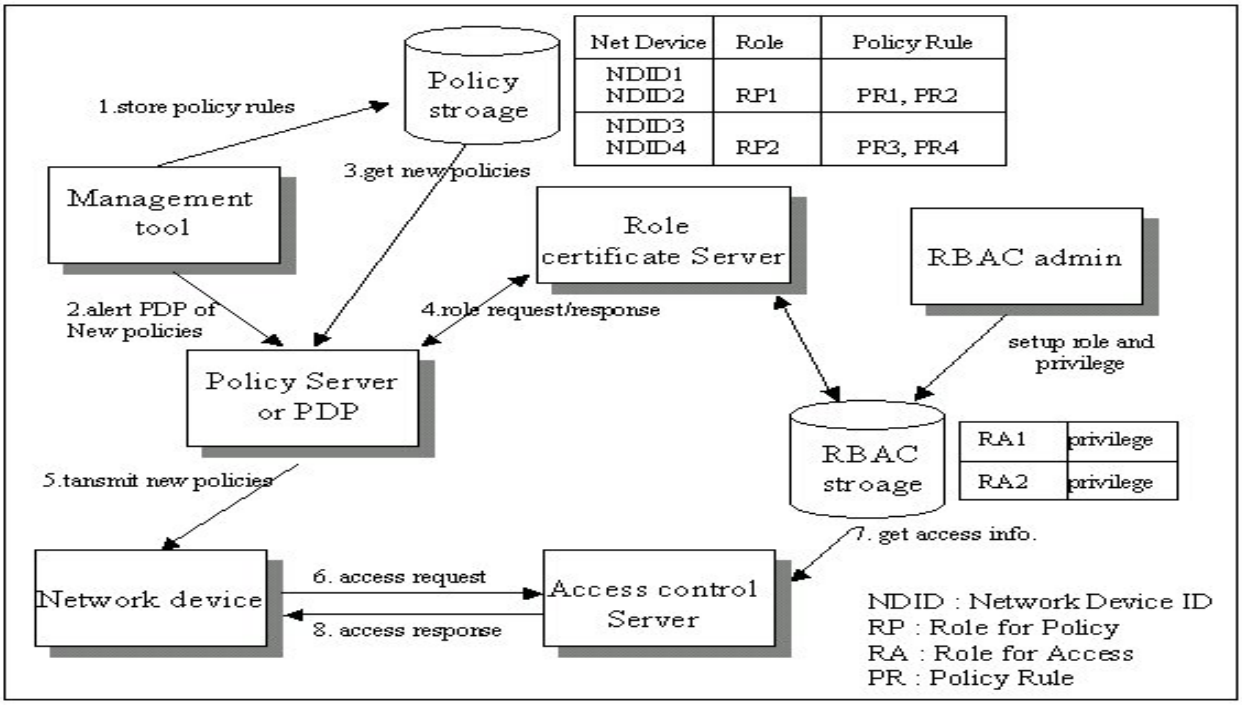

Fig. 3. Role & Policy based Network Security Management Framework

would be stored in policy repository. If new policy rules have been specified or existing policy rules have been modified then, they should be specified or modified for each and every individual network devices to which they apply. This is not be a serious problem for a small company, but as size and complexity of the company grows, managing policy rules becomes overhead. A more cohesive approach that reduces administrative overhead is our goal. Following we present Role & Policy based Network Security Management (RPNSM) model which supporting efficient management.

4.2 Role & Policy based Network Security Management (RPNSM) model

In RPNSM, there are two kinds of role: access_role, policy_role. Access_role is same to the role that used to control access like that described in section3. Policy_role play a interface role between policy rules and network devices. Policy role provide a way to bind policy rules to network devices without having to explicitly identify network devices across all network. Figure 5 depicts framework of RPNSM.

Network device, role certificate server, RBAC admin and access control server are same to components in figure 4. Additionally, Policy Server, policy storage, and management tool are added in RPNSM.

- Management tool: create and modified policies and notify PDP of changes in policies.
- Policy Server or PDP: provide policies of affected network devices and make policy decision.
- Policy storage: contain relations between network device, role, and policy rules.

Network management tool create and store new policies and notify policy server of creation of policy rule. And it also setup the relation of network device, policy_role, and policy rule. Then, policy server performs security management task after having process of access control like figure 4. There are some of advantages of using policy_roles when they play interface role between network device and policy rules. Even though existing policy rules are modified, it does not need to modify them for each and every individual network devices to which they apply. When new network device are installed, existing policy rules are applied to the new network device by assigning the relevant policy_roles to the new network device.

4. Conclusion

In this paper, we presented two kinds of model for network security management: network management model using RBAC and Role & Policy based Network Security Management (RPNSM). Each security service and tool is important aspects of security but the

effective and secure management of the tools is most critical in recently as size and complexity of the company grow. Role based access control is used to control an access to network device to increase the security of network management. This paper also presented Role & Policy base Network Security Management model that reduce the overhead of management in policy based networking. When network behaviors have been changed, RPNSM just performs a single update to the policy for the policy_role rather than configuring each of network components. In this paper, we do not comment the security of communications between network components. But the trusted channel between network components also should be considered.

References:

[1] Steven, Mark L., and Weiss, Walter J., "Policy-based Management for IP Networks", Bell Labs Technical Journal October-December 1999: 75-94

[2] http://www.ietf.org/rfc/rfc2753.txt

[3] Dave Kosiur, "Understanding Policy-Based Networking", 2001

[4] http://www.kb.cert.org

[5] David F. Ferraiolo, Ravi Sandu, and Serban Gavrila. "A Proposed Standard for Role-Based Access Control", http://csrc.nist.gov/rbac/

[6] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. "Role-based Access Control models",IEEE Computer, 29(2):38-47, February 1996.

[7] D. Ferraiolo, J. Cugini, and D. R. Kuhn. "Role-based Access Control: Features and motivations", In Annual Computer Security Applications Conference. IEEE Computer Society Press, 1995.