World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:1, No:10, 2007

Security Engine Management of Router based on Security Policy

Su Hyung Jo, Ki Young Kim, and Sang Ho Lee

***Abstract*—**Security management has changed from the management of security equipments and useful interface to manager. It analyzes the whole security conditions of network and preserves the network services from attacks. Secure router technology has security functions, such as intrusion detection, IPsec(IP Security) and access control, are applied to legacy router for secure networking. It controls an unauthorized router access and detects an illegal network intrusion. This paper relates to a security engine management of router based on a security policy, which is the definition of security function against a network intrusion. This paper explains the security policy and designs the structure of security engine management framework.

***Keywords*—**Policy server, security engine, security management, security policy

I. Introduction

THE intrusion of Internet is being increased, and the damage of intrusion affects public institutions, social infrastructures and financial institutions. A network security technology such as a virus vaccine, a firewall[1][2], an intrusion detection system, VPN[3] are required to handle Internet attacks. A conventional method of a network security is mainly implemented based on an individual security system having a single function, so that it is difficult to achieve internetworking between security systems and construct an information security infrastructure.

A router, a key component of the Internet, controls a data packet flow in a network and determines an optimal path to reach a destination. An error of the router or an attack against the router can damage an entire network. Since the router is connected to at least two networks and manages network traffic, the security is necessary to control of an unauthorized router access and an illegal network intrusion. Secure router technology has security functions, such as intrusion detection, IPsec[4] and access control, are applied to legacy router for secure networking.

Security management has changed from the management of security equipments and useful interface to manager. It analyzes the whole security conditions of network and preserves the network services from attacks. The targets of management are extended to backbone networks from enterprise networks. Security management solution collects intrusion detection event of IDS, makes a decision of appropriate response through the enterprise network. It collects flow based traffic information, analyzes the abnormal traffic.

ESM products are made as integrated security solutions in the world market. Domestic ESM products can collect 5,000 logs per second and guarantee error rate of response time within 2 hours per year. ESM products will be developed to weakness management system and real-time relationship analysis system. The products, which offer integrated security and interoperability of other company products, are needed in the future.

This paper relates to a method for security engine management for secure networking based on a security policy. Security policy is the definition of security function against a network intrusion. Security engine provides security functions of a packet filtering, an authentication, an access control, an intrusion analysis and an audit trail in the kernel region of router. It is capable of detecting a network intrusion and coping with an illegal network intrusion in real time.

The remaining parts of the paper are organized as following. Chapter 2 introduces policy based network management and related works. Chapter 3 addresses the security policy of security engine. Chapter 4 describes the security engine management framework. Finally, chapter 5 presents the conclusion of this paper.

II. Related Works

A. COPS

COPS (Common Open Policy Service) is describing policies and transferring and negotiating them around the network or among devices. If either the server or client is rebooted or restarted, the other would know about it quickly. COPS protocol uses a reliable TCP transport and provides an efficient transport of attributes and an efficient and flexible error reporting.

The COPS protocol provides message level security for authentication, replay protection, and message integrity. COPS can also reuse existing protocols for security such as IPsec or TLS to authenticate and secure the channel between the PEP and the PDP.

Su Hyung Jo is with Electronics and Telecommunications Research Institute, Daejeon, Korea (phone: 82-42-860-5499; fax: 82-42-860-5611; email: shjo@etri.re.kr).

Ki Young Kim is with Electronics and Telecommunications Research Institute, Daejeon, Korea

Sang Ho Lee is with School of Electrical and Computer Engineering, Chungbuk National University, Cheongju, Korea.

COPS open sources are COPS stack 1.4.0 by Vovida.org [8]. Vovida.org is a communications community site dedicated to providing a forum for open source software used in telecom environments. COPS stack is developed in C++. The stack is compliant with RFC 2748 and implements all of the functionality outlined in RFC except the support for IPv6 addressing scheme. In addition, the stack also contains implementation of COPS-PR.

B. The Trends of Network Security Technology

Security solutions have changed from individual security systems to integrated security solutions. Network security management has changed from a simple monitoring to a high performance network security management framework which operates intrusion detection, analysis, and response of attacks through the whole network. The trends of network security technology are unified threat management (UTM) appliance, ITSoC, and security module of network devices. UTM is integrated firewall, VPN, intrusion prevention, contents filtering into a network security device. Network security equipments are developed embedded devices for high speed hardware.

CISCO[10], Nortel Networks[11], and Enterasys[12] make security products, which are high speed security network equipments such as firewall, VPN, IDS of router and switch. 1700 series Modular Access Router of CISCO are access routers, which operate VPN, firewall, IDS. Other security solutions are Passport solutions of Nortel Networks, J-Protect of Juniper[9], and XSR-4000 Enterasys. Some companies have developed security chips of security functions. Software products are different from hardware in the performance of security solutions. Hardware products of IPS and firewall have 10sGbps speed.

III. Security Policy of Security Engine

Security engine has security functions, which are applied to legacy router for secure networking. The security engine has security policies, which are packet filtering policy, intrusion detection policy, access control policy, and VPN policy. It checks whether the packet through network interface is allowed or not, according to the packet filtering policy. Also, security engine detects and blocks a network attack by applying an intrusion detection policy. After detecting attack, security engine notifies alert manager of the attack. The detections of intrusion are not only signature based detections about known attacks but also suspicious traffic analysis and estimation of abnormal attacks.

Access control policy is definitions for preventing an unauthorized user and allowing an authorized user to access to the router. Only security manager has an authority to modify routing table of router by access control policy. Even if an unauthorized user discovers a password of a root by using a sniffing program and acquires a root authority, it is impossible to modify the routing table. As a result, the security of the router can be enhanced.

Table I shows packet filtering policy. This policy defines a drop or a pass the packet through the network interface.

The condition and the action of the packet filtering policy include the following:

TABLE I
Packet Filtering Policy

Name	Description
Prid	An integer index to uniquely identify an instance of this class
Priority	The priority of the packet filtering policy. This value is unique except '0'. The policy with '0' value has the highest priority
Protocol	Protocol [TCP(6), UDP(17), ICMP(1), Any(0)]
SourceIpAddress	The single IP address of a source host
SourceIpAddresMask	The mask of an IP address of a source host
DestinationIpAddress	The single IP address of a destination host
DestinationIpAddresMask	The mask of an IP address of a destination host
SourcePort	The port range, or single port number of a source host
DestinationPort	The port range, or single port number of a destination host
IcmpType	ICMP type value
IcmpCode	ICMP code value
TimePeriod	An overall range of start times and end time which a policy is valid. yyyymmddThhmmss/yyyymmddThhmmss
Action	The action for matched packets [Accept(1), Drop(2)]

*Condition
- Priority
- 5-tuple (Source IP, Destination IP, Source Port, Destination Port, Protocol)
- Time Period (Start Time, End Time)
- ICMP Type, ICMP Code

*Action
- Drop / Accept

5-tuple is source IP address, destination IP address, source begin and end port, destination begin and end port, and protocol. IP has 32bit address and mask address or 'Any' type. 'Any' means IP of packet doesn't care. Protocol is 'Any' type, 'TCP', 'UDP', and 'ICMP'. 'Any' means the protocol of packet doesn't care. The priority classifies the order of policy enforcement. If priority is '0', then this policy is first applied to router such as auto response of attack. Because several policies are auto response character, '0' of priority is overlapped. 'TimePeriod' is duration of policy lifetime. The format of 'TimePeriod' is 'NONE' or 'yyyymmddThhmmss/yyyymmdd Thhmmss'. The first date indicates the beginning of the range, while the second date indicates the end. They are separated '/'. If the 'TimePeriod' is 'NONE', then it means that the policy is installed immediately. If 'TimePeriod' is '20051208T120000 /20051209T120000', then it means that the policy will be installed at noon 8 December 2005, and will be removed at noon 9 December 2005.

Table II shows VPN policy. This policy defines security associations, which are how to protect the traffic, and what traffic to protect between host and gateway or end hosts.

VPN policy defines authentication and key negotiation of security associations between two end points of IPsec tunnel. 'Left_end' and 'Right_end' are IP of two end hosts. 'Protocol'

TABLE II
PACKET FILTERING POLICY

Name	Description
Prid	An integer index to uniquely identify an instance of this class
Policy	The action of packet process [Apply(1), Drop(2)]
Left_end	IP address of left end host
Left_private	The protected area with left_end host, IP_address/maskbit, ex) 12.23.22.0/24
Nexthop	IP address of first nexthop Gateway
Right_end	IP address of right end host
Right_private	The protected area with right_end host, IP_address/maskbit
Authby	Authentication method [Preshared key(1), Cert based RSA signature(2), RSA(3)]
Mode	Encapsulation mode [transport(1), tunnel(2)]
Protocol	IPsec protocol [AH(1), ESP(2)]
Keyingtries	The number of key trying
Ikelifetime	Phase 1 (ISAKMP) SA lifetime, unit is hour
Keylifetime	Phase 2 (IPsec) SA lifetime, unit is hour
LeftendCert	Left end Cert filename
RightendCert	Right end Cert filename
P1_prop	phase 1 proposal, ex) 3des-md5
P1_dh	phase 1 DH group [MODP768(1), MODP1024(2), MODP1536(5), MODP2048(14), MODP3072(15), MODP4096(16)]
P2_prop	phase 2 proposal, ex) 3des-md5
P2_dh	phase 2 DH group

is IPsec protocol, AH or ESP, between end hosts. If 'Authby' is 'Cert based RSA signature', then 'LeftendCert' and 'RightendCert' have to be defined.

IV. SECURITY ENGINE MANAGEMENT FRAMEWORK

The framework of security engine management has policy server, policy DB, COPS client, time controller, and alert manager. Fig. 1 is shown framework architecture.

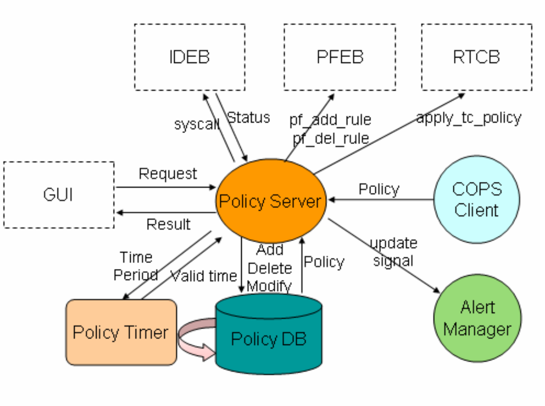


Fig. 1 The framework architecture of security management engine

Policy server stores the policy at DB and enforces the security policy to security router. The security policies are packet filtering policy, intrusion detection policy, trusted channel policy, and access control policy. The security policy is exchanged between COPS client and COPS server by COPS protocol. The policy is encoded by BER, because of data encoding. After decoding the policy, it is stored at GDBM (GNU Database Management) database. GDBM makes efficient search of policy and light-weight database. GUI, user interface, receives management information from policy server and displays security engine management.

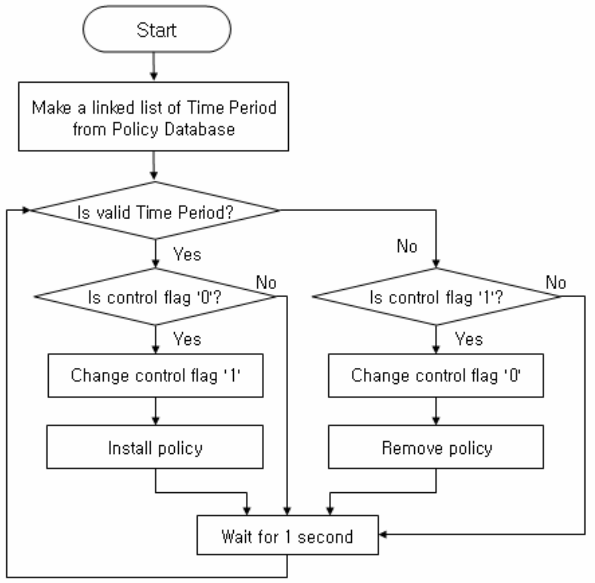


Fig. 2 The detailed flowchart of policy timer

Fig. 2 is a detailed flowchart for illustrating a process of policy timer. A process for installing or removing policy by timer is as following

(a) Timer makes a linked list of time period from policy DB. The linked list consists of prid, time period and control flag.

(b) Timer compares the current time with time period.

(c) If current time is in the range of time period in the step (b), timer compares control flag with '0'. Control flag means whether policy is installed or removed.

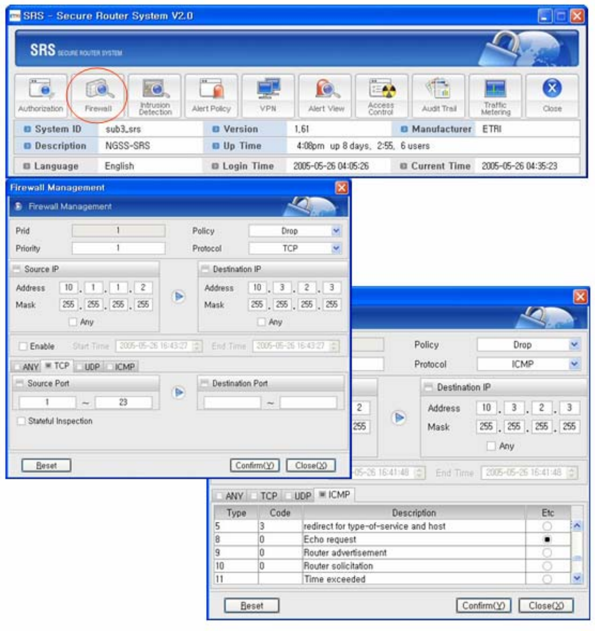
(d) If control flag is '0', then timer changes control flag '1' and install the policy. If control flag is '1', it means that policy is already installed and needs not install.

(e) If current time is out of the range in the step (b), timer compares control flag with '1'.

(f) If control flag is '1', then timer changes control flag '0' and remove the policy. If control flag is '0', it means that policy isn't installed and needs not remove.

(g) Timer checks the time of policy with current time every one second.

Fig. 3 shows the packet filtering policy of the router. Upper window is the GUI menu of Security engine management of router. The functions of GUI are Authentication, Firewall, Intrusion Detection, Alert Policy, VPN, Alert View, Access Control, Audit Trail, Traffic Metering and Close. Left window is firewall policy about TCP protocol. The packet of TCP protocol is dropped if source IP is 10.1.1.2, destination IP is 10.3.2.3, and source port is between 1 and 23. Right window is firewall policy about ICMP protocol. The packet of ICMP protocol is dropped if the packet is echo request.



System ID: sub3_srs | Version: 1.61 | Manufacturer: ETRI
Description: NGSS-SRS | Up Time: 4:08pm up 8 days, 2:55, 6 users
Language: English | Login Time: 2005-05-26 04:05:26 | Current Time: 2005-05-26 04:35:23

Firewall Management

Firewall Management

Prid: 1 | Policy: Drop
Priority: 1 | Protocol: TCP

Source IP — Address: 10 . 1 . 1 . 2 — Mask: 255 . 255 . 255 . 255 — □ Any
Destination IP — Address: 10 . 3 . 2 . 3 — Mask: 255 . 255 . 255 . 255 — □ Any

□ Enable — Start Time: 2005-05-26 16:43:27 — End Time: 2005-05-26 16:43:27

□ ANY ■ TCP □ UDP □ ICMP

Source Port: 1 ~ 23
Destination Port: ~

□ Stateful Inspection

Policy: Drop
Protocol: ICMP

Destination IP — Address: 10 . 3 . 2 . 3 — Mask: 255 . 255 . 255 . 255 — □ Any

End Time: 2005-05-26 16:41:48

□ ANY □ TCP □ UDP ■ ICMP

Type	Code	Description	Etc
5	3	redirect for type-of-service and host	○
8	0	Echo request	■
9	0	Router advertisement	○
10	0	Router solicitation	○
11		Time exceeded	○

Fig. 3 The packet filtering policy of the router

V. Conclusion

An error of the router or an attack against the router can damage an entire network. The security is necessary to control of an unauthorized router access and an illegal network intrusion. The security engine management of router, which is capable of optimizing the detection of intrusion and coping with an illegal network attack. It analyzes the whole security conditions of network and preserves the network services from attacks. This paper relates to a security engine management of router based on a security policy, which is the definition of intrusion detection, IPsec and access control, against a network attack. This paper explains the security policy and designs the structure of security engine management framework.

References

[1] Chris Hare and Karanjit Siyan, *Internet Firewalls and Network Security*. 2nd ed. New Readers, 1996.

[2] Dorothy E, Denning, *Information Warfare and Security*, Addison-wesley, 1999.

[3] Charlie Scott, Paul Wolfe, and Mike Erwin, *Virtual Private Networks*. O'Reilly, 1998.

[4] Naganand Doraswamy and Dan Harkins, *IPSec: the new security standard for the Internet, intranets, and virtual private networks*, Prentice-Hall, 1999.

[5] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, *The Common Open Policy Service Protocol*, RFC 2748, 2000. Available: http://www.ietf.org/rfc/rfc2748.txt

[6] S. Herzog, J. Boyle, R. Cohen, D. Durham, R. Rajan, and A. Sastry, COPS Usage for RSVP, RFC 2749, 2000. Available: http://www.ietf.org/rfc/rfc2749.txt

[7] K. Chan, J. Seligson, D. Durham, S. Gai, K. McCloghrie, S. Herzog, F. Reichmeyer, R. Yavatkar, and A. Smith, COPS Usage for Policy Provisioning, RFC 3084, 2001. Available: http://www.ietf.org/rfc/rfc3084.txt

[8] Vovida.org homepage. Available: http://www.vovida.org/

[9] http://www.juniper.net/

[10] http://www.cisco.com/

[11] http://www.nortelnetworks.com/

[12] http://www.enterasys.com/

[13] JDK homepage. Available: http://java.sun.com/

[14] Jakarta homepage. Available: http://jakarta.apache.org/

[15] J. N. Kim, K. S. Lee, C. H. Lee: Design and Implementation of Integrated Security Engine for Secure Networking. In *Proc. International Conference on Advnaced Communication Technology*, Feb. 2004.

Su-Hyung Jo is an engineer of Electronics and Telecommunications Research Institute(ETRI), Secure Operating System team. Her research interests are network security, policy-based network management.