ICIC Express Letters
Volume **2**, Number **4**, December **2008**
 ISSN 1881-803X
pp. **351–357**

DESIGN AND RESEARCH OF A LARGE-SCALE NETWORK ACCESS CONTROL SYSTEM WITH HYBRID ROUTER CONFIGURATION

Wei Jiang, Binxing Fang, Zhihong Tian, Hongli Zhang

School of Computer Science and Technology
Harbin Institute of Technology
Harbin, P. R. China
{jiangwei, tianzhihong}@pact518.hit.edu.cn

Xinfang Song

Beijing Jingbei Vocational Campus
Beijing, P. R. China

Received April 2008; accepted July 2008

Abstract. *The existing methods for network access control management are very complex and costly and are not sufficient to secure the large-scale and complex network. It is necessary to investigate a more efficiently network control technique for blocking sites with harmful information in real-time. This paper presents a new automatic hybrid router configuration (HRC) approach to access control, which combines the advantages of direct configuration (DC) method and routing diffusion configuration (RDC) method to simplify access control configuration in large-scale networks. The proposed HRC is a flexible, adaptable and affordable approach to block/unblock the harmful IP address. At the same time it is more scalable and less error-prone than manual and traditional configuration of all the AS border routers in a large-scale and complex network. A comprehensive network access control system (NACS) for large-scale with the hybrid approach is designed and implemented. Experimental results of the system are given to verify the theoretical analysis and to confirm its high efficiency.*
Keywords: Large-scale network, Access control, Router configuration, Diffuses routing, Network access control system

1. **Introduction.** The increasing number of people, organizations, and enterprises that install and subscribe to the Internet makes the security management an important issue [1]. Some organizations, institutions, companies, and countries seek to restrict Internet access from within their premises and territories. For instance, companies often restrict access to leisure sites in order to improve employee productivity; schools must filter the violent and sexually-explicit content so as to children can't browse them. In Australia, many groups and individuals have campaigned for government mandated ISP-based filtering and blocking of Web pages unsuitable for children. In early 2006 the Federal Labor Party (ALP) announced that they would implement mandatory ISP-filtering if elected [2].

Nowadays, access control configuration in large-scale network is a highly complex process that involves the manual configuration of a wide range of network devices including routers, VLANs and firewalls. However, in large-scale and complex network, there are many border routers and there is often nearly one hundred G bit traffic in the border router. ISPs often want to limit routing table size because overflow can cause the router to crash [3]. Traditional network access control methods are not sufficient to block sites with harmful information in real-time.

In summary, the requirements for an effective router configuration of large-scale access control are: (a) effective and timely router configuration for blocking harmful sites as

possible; (b) limiting routing table size of the border routers as possible; and (c) manageability and usability configuration for the administrators.

Our work aims to satisfy these requirements by presenting a new automatic hybrid router configuration approach to block the harmful IP address in large-scale network. Our approach is an extension of our lab's previous work [4,5] and it differs from the above studies. Compared with our previous work, the new automatic HRC approach to access control is presented, which combines the advantages of DC method and RDC method to simplify access control configuration in large-scale networks. What's more, A comprehensive network access control system for large-scale with the hybrid approach is designed and implemented.

The rest of this paper is organized as follows. In Section 2, a new automatic hybrid router configuration approach to block the harmful IP address is presented and analyzed. Section 3 designs and implements the NACS for large-scale with the hybrid router configuration approach. Section 4 discusses related work. Finally, Section 5 offers some concluding remarks.

2. **Hybrid Router Configuration Approach (HRC) for Network Access Control.** The main idea of our hybrid router configuration based on border routers of ISP is that using two mixed configuration (DC and RDC method) to modify the route table of some border routers. Therefore, the border routers can block and unblock the harmful IP address and prevent the harmful sites from establishing bidirectional communication with the internal hosts. The border router receives the offending traffic destined to the harmful IP address and then assigns the next-hop to be an address associated with the "null" route, or the address of a monitoring engine that can perform further analysis of the traffic.

The main advantages of this hybrid router configuration method are that (a) it causes less interference than pure DC method, (b) it is more efficient than pure DC method since some configurations are processed automatically, and (c) it is more exible and cheaper than pure hardware monitoring.

2.1. **Direct configuration (DC) method.** In DC method, configuration engine automatically queries the control policy database for the harmful IP address of block or unblock information, then process them and directly configures the static route table of corresponding border routers to block or unblock the harmful IP address.

The advantages of this method are quickly implementation of control policies and high PRI. However, a large ISP may have many border routers and the DC method may have low efficiency. ISPs often want to limit routing table size because overflow can cause the router to crash. This can be a particularly important issue for smaller ISPs which may have less expensive routers with less memory capacity. So we can use dynamic route protocol to route and diffuse the block IP addresses to border routers.

2.2. **Routing diffusion configuration (RDC) method.**

2.2.1. *The architecture of RDC.* The conceptual architecture for RDC method is given below in Figure 1. Here ISP0 is an ISP that applied network control policy. The configuration router can directly link with border or by linking one or multiple intermediary router. There are two manners for establishing routing diffusion link: (a) Special line, the advantages of which are high speed, stability and efficient, and the disadvantage of which is its cost is high; (b) The VPN connecting by IP tunnel, the advantage of which is that its cost is lower while the speed, stability and efficient of the manner are poorer than special line. We can adapt appropriate manner according to practice applies.

The configuration engine connects with the console of configuration router and configures the static route table to block the offending traffic. To be specific, when the

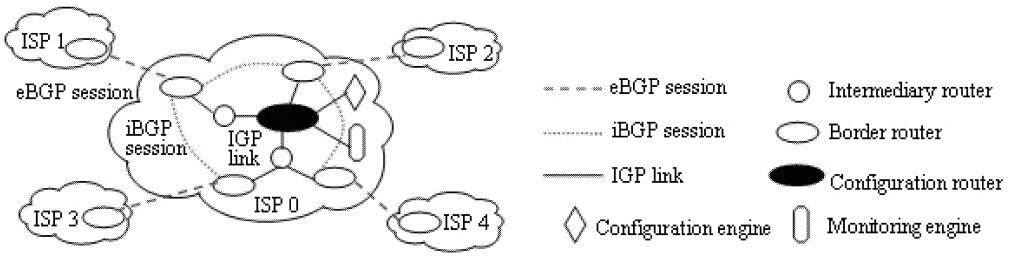


FIGURE 1. Conceptual architecture

configuration engine get the harmful IP address ip1 from the database, it will connect the console of configuration router and install a static blackhole route that assign the next-hop to be an address associated with the "null" route (a route which drops all traffic), or the address of a monitoring engine that can perform further analysis of the traffic. The static route can be diffused to other intermediary routers or border routers of the ISP. The border router receives the offending traffic destined to the ip1 and then assigns the next-hop to be an address associated with the "null" route, or the address of a monitoring engine. In final, the border router prevents the harmful sites from establishing bidirectional communication with the internal hosts. Vice versa, Configuration engine connects with the console of configuration router and configure the static route table to unblock the ip1.

2.2.2. *Selecting and configuration of routing dynamic routing protocols.* In most backbone networks, the routers participate in three different routing protocols: the internal Border Gateway Protocol (iBGP) that is used to propagate the information inside the AS, the Interior Gateway Protocol (IGP) that uses link-state information to learn how to reach other routers in the same AS, and the external Border Gateway Protocol (eBGP) that is used to exchange reachability information among routers in neighboring domains. In our design, as shown in Figure 1, we adapt eBGP to exchange reachability information among routers in neighboring ASes, iBGP to propagate the information inside the AS, and an IGP (such as OSPF) using link-state information to learn how to reach other routers in the same AS. In Figure 1, Solid lines correspond to physical links (IGP link) and dashed lines correspond to BGP sessions.

3. Design and Implementation of a Large-scale Network Access Control System.

3.1. **Design objectives.** Large-scale network pose special challenges for network access control because of their complexity, the variety of heterogeneous devices and users, and new modes of interactions with the system. What needed is a flexible, adaptable and affordable security solution, which provides greater autonomy. From our model, we obtain the following design goals for an access control system implementation: efficiency, scalability, manag-eability, usability.

3.2. **Functional architecture and components.** As Figure 2 shown in details, we now present the main building blocks of the NACS.

3.2.1. *User interface module.* User interface module runs in a separate machine and is an interface between users and the NACS. Administrators can fill harmful IP addresses and monitor the NACS' running condition by the user interface, such as configuration checking, device working, error and log information. Finally, administrators can query statistic analysis of the filter traffic from the monitoring engine.

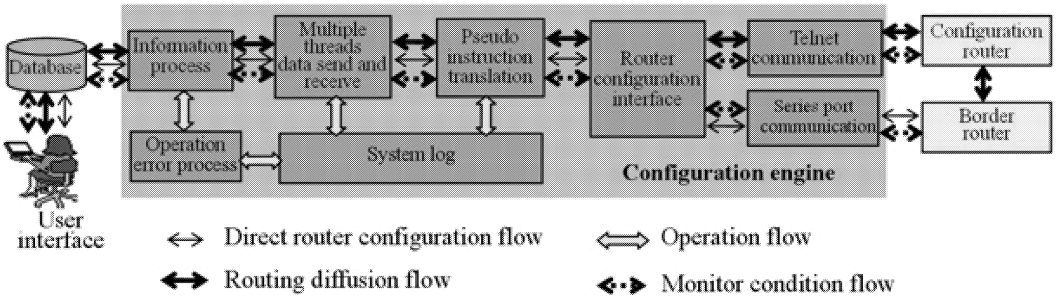


FIGURE 2. Functional architecture

3.2.2. *Configuration engine.* The configuration engine acts as a centralized controller that takes in configuration inputs and sends out configuration information to the configuration router and individual border routers. Configuration engine system is an important subsystem in the NACS and requires high speed, efficiency and security of data processing. We adapt multiple threads technology and the encryption and decryption mechanism to achieve above requirements. As Figure 2 shown, Configuration engine system is composed of eight function parts.

3.2.3. *Configuration router.* Configuration router acts as the diffusion of static route to other intermediary routers or border routers of the ISP by dynamic route protocol.

3.2.4. *Border router.* Border routers that reside at the edges of an AS can block and unblock the harmful IP address and prevent the harmful sites from establishing bidirectional communication with the internal hosts. The border router receives the offending traffic destined to the harmful IP address and then assigns the next-hop to be an address associated with the "null" route or the address of a monitoring engine. Some settings are necessary to consider: (a) we must forbid the border routers to promulgate route information to the configuration router and intermediary routers, namely the route is unidirectional. Bidirectional route among border routers can cause the route information to confuse; (b) we should set the diffusion routings form the configuration router with higher privilege in order to achieve effective network access control.

3.3. **System implementation and evaluation.**

3.3.1. *Qualitative and quantitative analysis.* Assume n is the total number of IPs to be blocked or unblocked once, V_1 is the time of configuration engine processes a configuration. V_2^i is the average time of transit a configuration on the ith communication link, $1 \leq i \leq M$, M is the total number of communication links. V_3^j is the response time of the jth router receives a configuration. $1 \leq j \leq N$, N is the total number of configuration or border routers. Then we have T, the time of configurations go into effect Equation (1).

$$T = \alpha * n * V_1 + T_2 + T_3 \tag{1}$$

Here α is the efficiency coefficient of configuration with parallel processes of configuration engine. And

$$T_2 = \max(n * V_2^1, n * V_2^2, \cdots, n * V_2^M) \tag{2}$$

$$T_3 = \max(n * V_3^1, n * V_3^2, \cdots, n * V_3^N) \tag{3}$$

In ideality, $\alpha \to 1/n$. From above, we can found that only parameter V_1 is can be controlled. Take V_3^j for example, the difference of response time between HUAWEI AR4600 and HUAWEI NE05 is very much. Sometime the response time is 10 second per IP; sometimes is 1 second per IP. The following experiments will prove that the response time has something with the load of routers.

3.3.2. *Simulation experiment and result.* The network topology of our experiments is shown in Figure 3. There are a configuration engine, a configuration router, monitoring engine, and two border routers. Some important host information is given in Table 1.

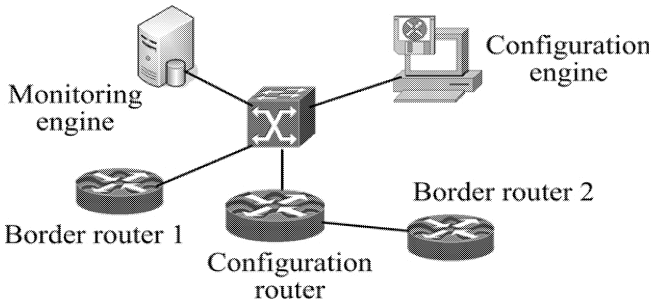
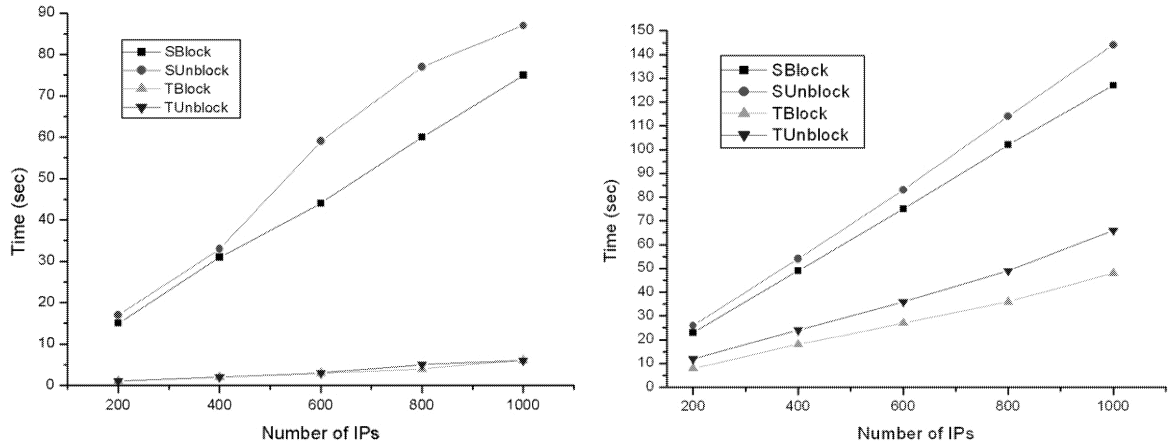


FIGURE 3. Simple network topology

TABLE 1. Some configuration information

Entities	Configuration information	IP address
Configuration engine	CPU:2.4G∗2, RAM:4G, Disk:100G, RedHat Linux 7.2	10.10.60.1
Monitoring engine	CPU:2.0G, RAM:1024M, Disk:60GB, Windows	10.10.60.2
Configuration router	HUAWEI AR4680, OSPF, area 0	10.10.60.3
Border routers	HUAWEI Quidway 3600, OSPF, area 0	10.10.60.4, 10.10.60.5

We measured the throughput of the DC and RDC approach using the time of configurations going into effect. For the DC, the configuration engine connects with the border router by the series port communication to block or unblock IP addresses. For the RDC, configuration engine connects with the configuration router by TELNET communication and configure IP addresses. Because the routing diffusion speeds in the same area is very high and it much depends on the network conditions, we only measure the time of configurations going into effect on the configuration router. Simulation results on different conditions as shown Figure 4.



(a) The load number $N = 0$ (b) The load number $N = 15000$

FIGURE 4. Simulation results

Figure 4 shows the simulation results on two different load conditions. Figure 4(a) shows the time property of series port configuration block(SBlock), series port configuration unblock (SUnblock), TELNET configuration block (TBlock) and TELNET configuration block (TUnblock) with the load number $N = 0$ in the router. Figure 4(b) shows the time property of different configuration methods with the load number $N = 15000$ in the router.

Experimental and practice results of the system are given to verify the theoretical analysis and our design objectives.

4. **Related Work.** The network access control methods are mainly access control list based routers [6,7] and firewalls [8].

A lot of network devices have their access control list function, such as routers. Jun Gao [6] presented a set of security mechanisms based on access control lists that are used to check all active extensions' operations that may affect the use of link bandwidth, or may involve access to user traffic. In their 4D architecture, Rexford *et al.* [7] argue that the decentralized routing policy, access control, and management have resulted in complex routers and cumbersome, difficult-to-manage networks.

Today, many security technologies other than access control, such as intrusion detection, audit and encryption, are integrated into firewalls. In the concept of the active firewall proposed by [8], a firewall is a set of systems that comprise traditional firewall, vulnerability scanner, antivirus tool, encryption facility, and even PIU server.

Our HRC is better than ACL and firewall in many aspects such as efficiency, stability, configuration rule capacity, scalability and manageability. Table 2 shows the different characteristics among the above-mentioned three access control methods in the large-scale network. On one hand, it is a cumbersome work for the security administrator to configure the large number of rules in multiple router or firewalls distributed around the perimeter. On the other hand, with the revolutionary increase and the requirement for high bandwidth, the decrease of throughput brought by ACL and firewalls can not be ignored. Overfull access control rules of ACL or firewalls can result in some problems such as performance decreasing, asymmetric routing and multicasting problems, etc. [9].

Table 2. Characteristics compare of three network control methods

Item	**ACL**	**Firewall-based**	**HRC**
Efficiency	Low	Low	High
Stability	Good	Good	Better
Configuration rule capacity	Medium	Medium	Large
Scalability	Poor	Poor	Good
Manageability	Poor	Poor	Good
Human Interaction	Manual	Manual	Autonomous

5. **Conclusions.** This paper presents a new automatic hybrid router configuration (HRC) approach to simplify access control configuration in large-scale networks. Unlike traditional access control configuration approaches, HRC is a flexible, adaptable and affordable approach to block/unblock the harmful IP address. And we deigned and implemented a comprehensive network access control system (NACS) with the HRC method for large-scale to reduce the network management load. This significantly improves scalability and performance while minimizing the manual intervention. Practices prove that the NACS not only meets the actual demand but also has some advantages, such as high efficiency, scalability, manageability and brilliant performance.

Acknowledgment. This paper is supported by the National High-Tech Research and Development Plan of China under Grant No.2007AA01Z406, No.2007AA01Z442. We also thank anonymous reviewers for their constructive suggestions.

REFERENCES

[1] M. Pilgermann, *et al.*, Security in heterogeneous large scale environments using grid technology, *International Journal of Innovative Computing, Information and Control*, vol.1, no.4, pp.715-725, 2005.

[2] *Internet Content Filtering and Blocking*, http://www. efa.org.au/Issues/Censor/cens2.html, 11, 2008.

[3] D. Newman, Super firewalls, *Data Communications*, vol.28, no.5, pp.51-61, 1999.

[4] W. Jiang, H.-L. Zhang, Z.-H. Tian, *et al.*, A game theoretic method for decision and analysis of the optimal active defense strategy, *Proc. of the 2007 International Conference on Computational Intelligence and Security*, pp.819-823, 2007.

[5] G. Liu, X.-C. Yun, B.-X. Fang, M.-Z. Hu, A control method for large-scale network based on routing diffusion, *Journal of China Institute of Communications*, vol.24, no.10, pp.159-164.

[6] J. Gao and P. Steenkiste, An access control architecture for programmable routers, *Proc. of the 2001 IEEE Open Architectures and Network Programming*, Alaska, pp.15-24, 2001.

[7] A. Greenberg, G. Hjalmtysson, D. A. Maltz, *et al.*, A clean slate 4D approach to network control and management, *ACM SIGCOMM Computer Communication Review*, vol.35, no.5, pp.41-54, 2005.

[8] Network Associations Corp., *The Active Firewall: The End of the Passive Firewall Era*, http://www.nai.com/nai-Iabdasp-sethetwork-security.asp.

[9] R. Braden and D. Clark, *Report of IAB Workshop on Security in the Internet Architecture*, RFC1636, February 8-10, 1994. http://www.ietf.org/ rfc/rfc 1636.txt.