

<http://ansinet.com/itj>

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSI*net*

Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Implementation and Evaluation of the Live-CD Based Authentication Gateway

Jian-Bo Chen

Department of Information and Telecommunications Engineering, Ming Chuan University,
5 De Ming Rd, Gui Shan District, Taoyuan County 333, Taiwan

Abstract: The authentication is an important function in network security. For security issue, all the hosts must be authenticated in order to connect to the Internet. In this study, a Live-CD is used to implement an authentication gateway. This gateway is implemented according to Open Source and integrated all the functions in only one CD, so that the cost can be minimized. The performance evaluation is also shown in this study to verify that the proposed solution is practicable.

Key words: Authentication gateway, Live-CD, security

INTRODUCTION

Due to the popularity of Internet, network security issue is more and more important (Wu, 2010). In order to provide wired or wireless access in the public environment, an authentication mechanism is necessary for users to connect to the Internet (Cheng and Meinel, 2009). The authentication mechanism receives the user account and password, verifies the availability for Internet access and stores the records into the access logs. Then the user can use his own laptop or smart phone to access the Internet (Kehe *et al.*, 2009).

Beside to the public environment, the campus network also provides the wireless access for teachers and students. The teachers can use wireless for researching or teaching and learning purposes. The network administrator in campus must provide an authentication mechanism for wireless access (Gao *et al.*, 2011). How to build a cost-effective authentication mechanism is a challenge for the campus network administrator (Venkatesan and Manoharan, 2012).

There are many commercial products that implement the authentication gateway such as Cisco system, Aruba Network, Bluesocket and Cipherium System. But these solutions are too expensive for the campus to implement authentication. In this study, a cost-effective solution is used to implement the authentication gateway which is implemented by Open Source and can be integrated in only one CD. In this proposed solution, the network administrators can easily to build the authentication gateway in their network environments.

This proposed solution is implemented by a Live-CD. The original Live-CD is revised because some additional programs must be installed. An administrative web page is also constructed in the Live-CD. The revised Live-CD acts as the role of authentication gateway which

integrated the IPTables, DHCP server, NAT, MySQL, Apache, SSL, etc. The PHP and shell script are also used to integrate the system and data. When the authentication gateway is built, the performance is also evaluated (Hassan and Sailan, 2011). Different hardware specification, different number of concurrent requests and different download file size are used to compare the response time (Baklizi *et al.*, 2012). The experimental results show that this solution is practicable for campus to implement the authentication gateway (Liao *et al.*, 2005). There are many solutions to implement the authentication gateway like; research paper and commercial products.

There are many research paper proposed authentication gateway solution (Meng, 2011). Wu (1993) proposed the designing and implementing for public wireless network accounting system. Chen (2006) proposed the study and implementing for AAA-based dynamic firewall. These kinds of researches implement the authentication systems that are practical for the campus network.

The Bluesocket designs the authentication gateway for organization and campus used. It provides remote management, inter-operation, quality of service and security issues. The main functions include NAT, DHCP, authentication, multiple encryption mechanism, bandwidth management, role-based policy control, intrusion prevention, virus protection, etc. The second commercial product is Cipherium System. Its product is designed as two-tiered architecture. The front end is called NAM (Network Access Manager), which manages the user traffic. The back end is called NCS (Network Control Server), which controls the policies. The main functions include NAT, DHCP, Packet Filter, IPSec, VPN, System protection, accounting system, etc.

Table 1: Comparison of authentication gateway

	Bluesocket	Cipherium	(Wu 1993)	(Chen, 2006)
Authentication method	Multiple	Multiple	Radius	Radius
QoS	Yes	Yes	No	No
VLAN	Yes	Yes	No	No
Price	High	High	Low	Low
IPS	Yes	No	No	No
VPN/IPSec	Yes	Yes	No	No
Log size	Limited	Limited	Unlimited	Unlimited
Configuration	Complex	Complex	Easy	Complex
Setup	Easy	Easy	Complex	Complex
Session limitation	Depend on price	Depend on price	Unlimited	Unlimited

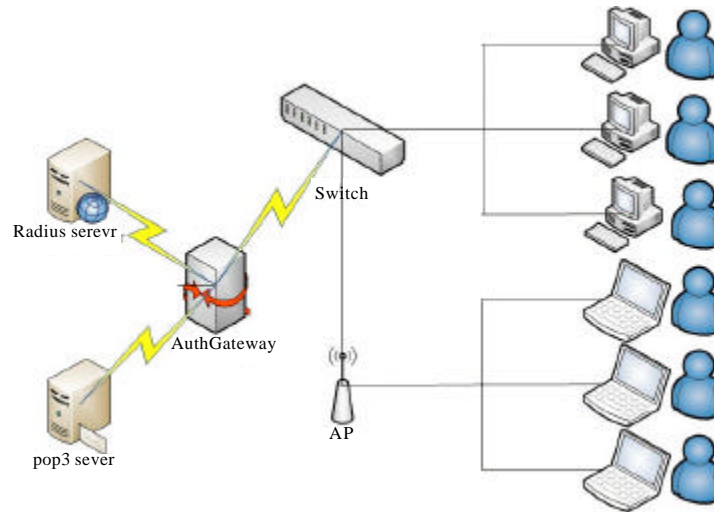


Fig. 1: Authentication gateway architecture

There are also some commercial products such as Cisco System and Aruba Networks. But these two products are too expensive so that they will not be compared in this study.

The comparison of relative authentication gateway: The authentication gateway, including commercial products and research papers, are compared in Table 1. The commercial products must support multiple authentication methods so that they are suitable for different organizations (Senan *et al.*, 2011). Besides, their management and transmission are more secure than others (Yan and Wang, 2012). But the configurations are more complex and the prices are more expensive. The concurrent session number is depending on the price. The proposed solutions by research papers are cost-effective and are designed by the specific network environments. But they need more time to implement and adjust (Jain, 2008).

SYSTEM IMPLEMENTATIONS

The operation system is Linux Live-CD and all the other software is integrated with this Live-CD. This

software includes DHCP, NAT, Firewall, Web Server, MySQL and PHP. The system implementation is consists of four parts, including authentication methods, IPTables implementation, Live-CD building and saving configuration files.

Authentication methods: There are two popular authentication methods, including IEEE 802.1x and web-based authentication (Safdar *et al.*, 2011). When the 802.1x is adopted, all the clients and all the network devices must enable this function, so 802.1x is hard to deploy in campus network. The proposed authentication implementation adopts web-based method. In order to avoid the security issue, the system also implements SSL encryption so that the username and password can be protected.

In web-based authentication method, the authentication gateway must install in the place where all the clients connect to the Internet. The authentication architecture is shown in Fig. 1.

When the client opens the browser and enter an URL, the authentication gateway will redirect this request to the authentication web page. The username and password are required for this authentication page. The username and

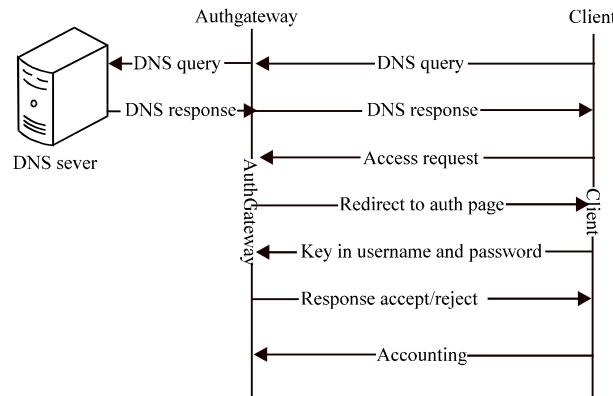


Fig. 2: Authentication processes

password are sent to the RADIUS server or POP3 server. If the username and password are correct, then the client can connect to the Internet.

IPTables implementation: In order to redirect the user request to the authentication page and limit the user connection, IPTables is deployed in the authentication gateway (Raza *et al.*, 2004). The process of authentication and relative IPTables commands are shown in Fig. 2 and are described as below:

- The authentication gateway only allow DNS request/response packet so that the name resolution can be success
- The authentication gateway redirects the user request by the following command, where 192.168.1.1 is the IP address of authentication gateway
- # IPTables-t nat -A PREROUTING -i eth0 -p tcp-dport 80 -j REDIRECT -to 192.168.1.1
- When the user enters the correct username and password, the authentication gateway will open the Internet access for that user. The IPTables command is shown as below, where 192.168.1.10 is the IP address of that user
- # IPTables -A INPUT -i eth0-p tcp-s 192.168.1.10-j LOG ACCEPT

Live-CD building: For the purpose of fast building and installing the authentication gateway, the Linux Live-CD is used as the operating system. The Live-CD is a CD that can boot up the operating system without hard disk. All the operating programs are store in the CD-ROM, so it can easily to re-build another gateway when needed. The original Live-CD only boot up the operation system. Thus, some software must be installed in this Live-CD,

such as DHCP, IPTables, NAT, etc. Then the revised Live-CD must be re-built. The re-build processes are described as below:

- Download all the needed software
- Make a directory named live, copy the Live-CD ISO file into this directory
- Mount the ISO file to mnt
- Make another directory named extract-cd
- Copy the contents of ISO files to extract-cd directory
- Use the default configuration to install the software into the live directory
- Modify the /etc/rc.local file in the live directory
- Remove the unnecessary temporary files and unmounts the mounted devices
- Build my own Live-CD ISO file
- Burn the ISO file into the CD-ROM

Saving configuration files: Because the Live-CD is read-only, the customized configuration files cannot be saved in this CD-ROM. In order to solve this issue, this study uses USB storage to save the configuration files. After loading the operation system, the Live-CD will check the USB storage to load the configuration files. If the USB storage does not exist or there are no configuration files, the system will use the default values to boot up.

In the step 7 of Live-CD building processes, when the rc.local is modified, the Live-CD adds a shell script so that the script can be executed when system booted. Table 2 is an example of the shell script. In this script, the configuration file is read and the network address is set. Then the DHCP server is enable depend on the configuration file. When the configuration setting is modified, the values will be saved in the USB configuration file. The example for configuration file is shown in Table 3.

Table 2: Example for shell script

```
#!/bin/sh
./media/disk/usb.txt
sudo ifconfig eth0 $eth0IP netmask $eth0netmask
sudo route add default gw $eth0Gateway
sudo ifconfig eth1 $eth1IP netmask $eth1netmask
sudo route add default gw $eth1 Gateway
sudo cp -rf /media/disk/dhcp.conf /etc/dhcp3/dhcpd.conf
if ["$DHCPStat" = "1" ]; then
    sudo /etc/init.d/dhcp3-server start
elif ["$DHCPStat" = "2" ]; then
    sudo /etc/init.d/dhcp3-server stop
else
    echo "Input 1 or 2"
fi
```

Table 3: Example for configuration file

```
eth0IP = 192.168.1.1
eth0netmask = 255.255.255.0
eth0Gateway = 192.168.1.254
eth1IP = 192.168.2.1
eth1netmask = 255.255.255.0
eth1 Gateway = 192.168.2.254
DHCP condition (1 = start, 2 = stop)
DHCPStat = 1
```

Experimental method: In order to evaluate the performance of Live-CD authentication gateway, the twenty clients download the files whose size is 250 kB, 500 kB, 750 kB and 1 MB. In addition, each of the twenty client issues 20, 40, 60, 80 and 100 download request simultaneously. The download time are compared in next section.

In the experiment, the twenty clients install a test program named test.sh. This program will download a file from file server periodically. The downloaded file contains a variable declared as sc. When sc equals to 0, the experiment will not start. When sc equals to 1, the experiment will start. Thus, the start time of experiment can be easily controlled. When the experiment starts, the client runs another shell script, named time.sh, which use wget to download the file from file server to evaluate the performance. When finishing the download, these clients run another shell script, named record.sh, which inserts the downloaded information and download time to database. When all the information are stored in database, the performance evaluation can be easily done by database operation. The experimental processes are shown in Fig. 3.

Experimental environment: In the experiments, twenty personal computers are used as the clients that will connect to Internet via the authentication gateway. Two different specifications of personal computers are used as the authentication gateway to evaluate the performance. All the twenty clients and two authentication gateways use the Ubuntu 10.10 as their operation system. In order to collect the experimental results, a file server is used to store the experimental results and some experimental

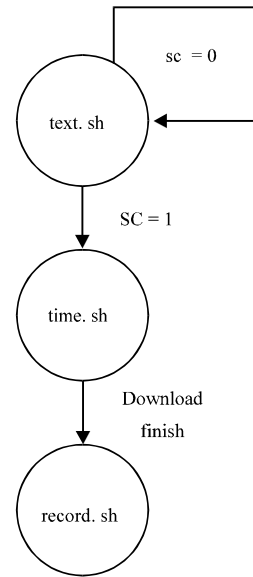


Fig. 3: The experimental processes

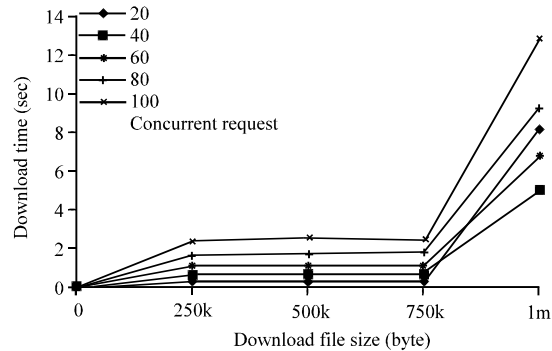


Fig. 4: The comparison of download time

Table 4: Experimental hardware specification

	Authentication gateway-1	Authentication gateway-2	Clients	File sever
CPU	Intel Pentium 41.6 GHz	Intel Core2Duo 1.86 GHz	Intel Core2Duo 1.86 GHz	Intel Core2Duo 1.86 GHz
Memory	1 GB	2 GB	2 GB	2 GB
Hard disk	120 GB	160 GB	160 GB	1 60 GB
Number	1	1	20	1

parameters. The hardware specifications are shown in Table 4.

Experimental results: In the first experiment, the average download time is compared when the download file size and concurrent requests are varied. When the download file size increased, the download time increased; when the concurrent requests increased, the download time also increased. The experimental results are shown in Fig. 4. When the download file size is 750 kB, the concurrent request number does not influence the download time,

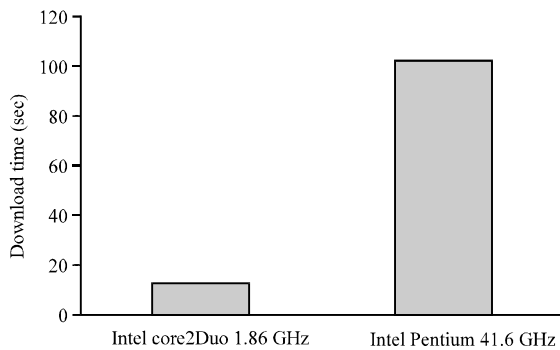


Fig. 5: The comparison for different hardware specification

they are all below three second. When the download file size is 1 MB, the concurrent request number has significant influence to the download time.

In the second experiment, the performance for different specification of hardware are compared. In this experiment, the twenty clients download 1 MB file size, and the concurrent request number is 100. The download time is compared when the hardware specification is different. If the authentication gateway is Core2Duo with 2 GB RAM, the download time is about 13 sec But if the authentication gateway is Pentium 4 with 1 GB RAM, the download time is increased to 102 sec, as shown in Fig. 5. The experimental results show that the hardware specification has the most influence to the performance.

CONCLUSION

In this study, the Ubuntu Live-CD is used for implementation of authentication gateway. The management and authentication functions are also implemented in this gateway. When users connect to Internet, the authentication gateway will pop up an authentication page for users to enter their username and password. Once the authentication processes are completed, the users can connect to Internet.

The implementation processes are also described in this study. It is easy to implement the cost-effective authentication gateway. The performance is also compared to verify that the proposed implementation is practicable. Even when there are twenty users concurrent download one hundred 1MB file size, the download time is only 13 sec. This proves that the proposed authentication gateway can afford heavy traffic.

REFERENCES

Baklizi, M., H. Abdel-Jaber, S. Ramadass, N. Abdullah and M. Anbar, 2012. Performance assessment of AGRED, RED and GRED congestion control algorithms. *Inform. Technol. J.*, 11: 255-261.

Chen, J., 2006. The study and implementing for AAA-based dynamic firewall. Master Thesis, Shih Hsin University.

Cheng, F. and C. Meinel, 2009. Design of Lock-keeper federated authentication gateway. *Proceeding of International Conference on Advanced Communication Technology*, February 15-18, 2009, Phoenix Park, pp: 1041-1046.

Gao, H., S. Wang and H. Lu, 2011. Local positioning systems for mobile devices based on ontology. *Inform. Technol. J.*, 10: 168-174.

Hassan, R. and M.K. Sailan, 2011. End-to-end baseline file transfer performance testbed. *Inform. Technol. J.*, 10: 446-451.

Jain, R., 2008. *The Art of Computer Systems Performance Analysis*. Wiley India Pvt. Ltd., India, ISBN:8126519053, Pages: 716.

Kehe, W., Z. Tong, L. Wei and M. Gang, 2009. Security model based on network business security. *Proceedings of International Conference on Computer Technology and Development*, November 13-15, 2009, Kota Kinabalu, pp: 577-580.

Liao, H.C., Y.W. Ting, C.M. Chen and C.C. Yang, 2005. A performance comparison of Ad hoc routing protocols based on ant mobility model. *Inform. Technol. J.*, 4: 278-283.

Meng, B., 2011. Automatic verification of deniable authentication protocol in a probabilistic polynomial calculus with cryptoverif. *Inform. Technol. J.*, 10: 717-735.

Raza, M.A., M. Omer, S.H. Khiyal and I.A. Gondal, 2004. Component based programming model for linux. *Inform. Technol. J.*, 3: 12-16.

Safdar, S., M.F. Hassan, M.A. Qureshi and R. Akbar, 2011. Effective methods for secure authentication in vulnerable workflows using nxn passwords. *Inform. Technol. J.*, 10: 1161-1169.

Senan, S., A.H.A. Hashim, A.S. Rashid and J.I. Daoud, 2011. Evaluation of nested network mobility approaches. *J. Applied Sci.*, 11: 2244-2249.

Venkatesan, S. and C. Manoharan, 2012. Access point selection for fair load balancing in wireless LAN. *Inform. Technol. J.*, 11: 283-288.

Wu, B., 1993. Designing and implementing for public wireless network accounting system. Master Thesis, Yuan Ze University.

Wu, C., 2010. The problems in campus network information security and its solutions. *Proceeding of 2nd International Conference on Industrial and Information Systems*, July 10-11, 2010, Dalian, pp: 261-264.

Yan, R. and Y. Wang, 2012. Hurst parameter for security evaluation of LAN traffic. *Inform. Technol. J.*, 11: 269-275.