2011 International Conference on Network and Electronics Engineering
IPCSIT vol.11 (2011) © (2011) IACSIT Press, Singapore

Designing the Network Access Control using Reverse VPN

Thananchai Khamket, Thawatchai Chomsiri, Patchayakorn Sripara, Mayta Swatpong
Faculty of Informatics, Mahasarakham University, Thailand
thananchai.k@msu.ac.th, thawatchai@msu.ac.th, deathnote_mix@hotmail.com, swatpong@hotmail.com

Abstract. The main problem of NAC (Network Access Control) is the bypassing authentication using MAC/IP cheating. Hackers will change their MAC/IP address to the MAC/IP address of authenticated users. After that, they will be able to access network resources including internet link. This research proposes a method for resolving this problem. We propose replacing NAC with VPN server and using 'Reverse VPN' method that VPN servers have to be placed between unauthenticated zone and the internal network (DHCP server will be placed on unauthenticated zone). When clients connect to the unauthenticated zone's network, they will receive an IP address that is not yet allowed by firewall. In this phase, they cannot access the resources located in the internal network including internet. Users must authenticate with the VPN server by using username and password. If the authentication is successful, they will receive secondary IP address and be able to access the resources located in the internal network (including internet). This secondary IP address is allowed by firewall. We have tested this method and found that if hackers cheat NAC by spoofing MAC and IP address, they will not be able to access the internal network. After the experiment, the result has shown that this method can prevent NAC cheating (with MAC/IP spoofing) while the network speed is still fast.

Keywords: Network Security, Reverse VPN, NAC, Network Access Control, MAC spoofing

1. Introduction

NAC: Network Access Control [1] is an important network device. It is used for authenticating the users with username and password before they are able to access the internal network and resources. The main trick of the NAC is, it will remembers MAC address of authenticated users before allowing the packets associated with recognized MAC addresses to pass the NAC.

Nowadays, NAC is facing a big problem. Hackers [2] are able to cheat the protected network by using MAC spoofing technique. They begin with scanning MAC address of the running computers (authenticated MAC address) and then change their MAC address [3] to be authenticated MAC address. Finally, hackers can access network resources without any authentication step. Moreover, hackers can do illegal activities such as hacking the internet web-sites using victim's identity. Hacking evidences recorded in a log file of the target web-sites will point to an innocent user not the hackers. All brands of NAC devices are vulnerable to this kind of attacking. The computer networks of governments, universities and private companies are facing security risks. We realize this problem and try to find a solution. We have designed a model and methodology for preventing this cheating. Moreover, we have tested our solution and we found that our method can solve this problem effectively.

2. Backgrounds and Related works

VPN: Virtual Private Network [4] was designed for the secure communicating by creating a tunnel across the public networks. There are 2 main types of VPN structure, 'Client to Site' and 'Site to Site' VPN. The first one, outdoor users are able to connect their office network remotely. The second one is often used for connecting branch offices.

‘Client to Site’ VPN, users need only 3 things for logging into the network. They consist of VPN Server’s IP Address, username, and password. After logging in, user will obtain an additional IP address. This IP address is used for accessing office network such as IP address of ‘B’ network in Fig 1. After that, authenticated users will be able to access internal network. They can print a document using office’s printers, they can access the internal database, or transfer files from/to shared folders located on the office’s computers. VPN-client and VPN-server programs are available on Windows XP, Vista, Windows 7, and Linux. Using VPN, administrators have to start VPN service on VPN server, and then users can access it. Fig-1 shows the use of VPN in the normal method.

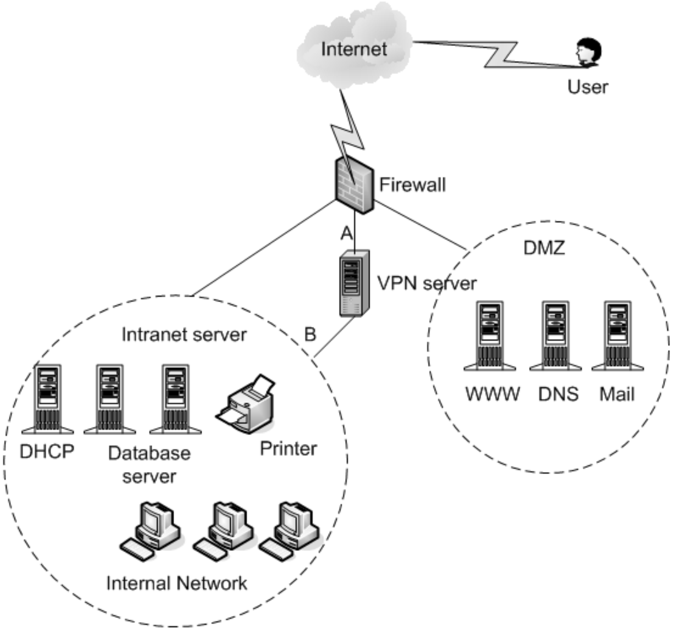

Fig. 1: Using VPN in the normal method.

3. Designed Model

In this research, we assigned the VPN to works as NAC. In the first step, all users were in unauthorized zone (see Fig 2). In the second step, users had to log in VPN server using VPN client software installed on the users’ computers. Users had to enter VPN server’s IP address, username, and password.

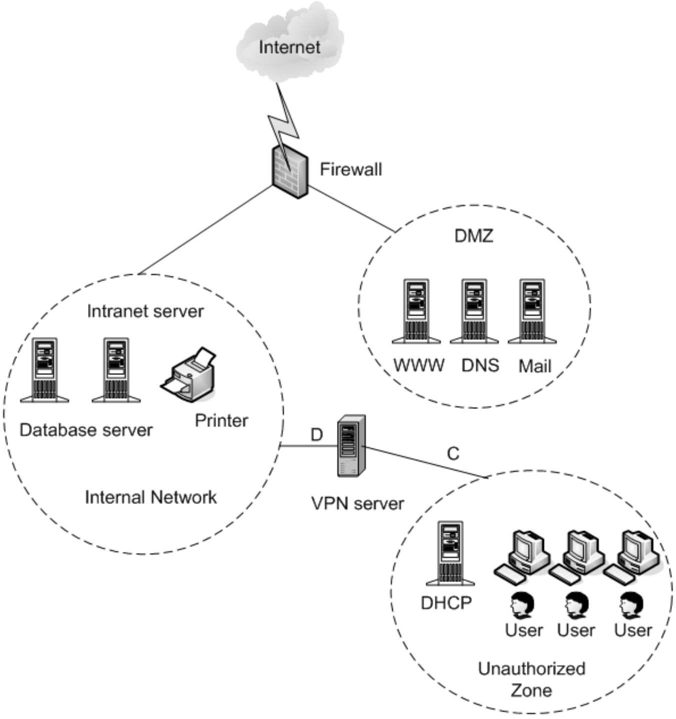

Fig. 2: Using reverse VPN as NAC.

In the third step, VPN server would authenticate the users and give secondary IP address to only authorized users ('D' network IP addresses that are allowed by firewall to accessing to internet and DMZ). Finally, authenticated users would be able to access the resources in the internal network including the internet.

In this model, DHCP server [5] was in unauthorized zone. Although hackers could obtain IP address from DHCP server directly, they could not access the internal network. They could not access the internet as well because they did not have 'D' network IP address. If hackers changed their MAC address to be an authenticated users' MAC address, they would still be unable to access the internal network because the victim's IP address they obtained was an unauthorized zone's IP address.

Although hacker's MAC/IP address matched with authenticated user's MAC/IP address, accessing internal network still needed to use 'D' network IP address (Fig. 2). Although hackers changed their IP address to 'D' network IP address directly, they were still unable to access internal network because physically, they were still connecting to a switch device placed on the unauthorized zone not the internal network. As you can see, VPN connecting method in our design (Fig 2) is opposite the normal method (Fig.1). Because of connecting to VPN in opposite side, we call this method 'Reverse VPN'. Reverse VPN can work as NAC properly. Administrators can create user accounts on VPN server or RADIUS server (for the large scale). Authenticating and logging can be processed on both VPN Server and RADIUS Server upon our configuration. In a large network, logging should be deployed on a dedicated log server.

Moreover, we found some advantages from this method. By default, reverse VPN could prevent data sniffing because all IP address would communicate within VPN channel which used data encryption scheme. Therefore, this method could help to solve the problem that involved with the data capturing [6] such as cookie sniffing [7] and session ID sniffing. This method would lead to prevention of session hijacking [8] as well.

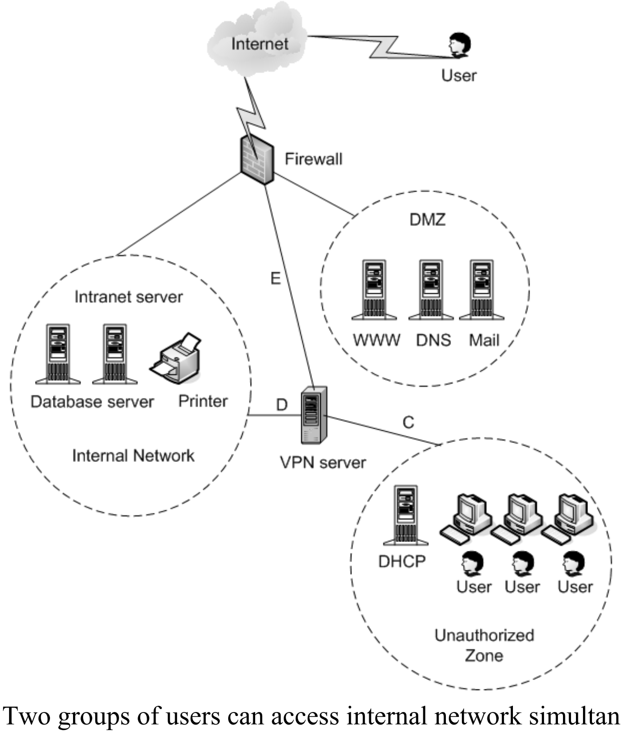

Fig. 3: Two groups of users can access internal network simultaneously.

We have modified our model to be a more flexible model in order for outdoor users to be able to access office network. We added the third network interface to VPN server (see Fig 3). External users were able to access the internal network by entering VPN server's IP address (in 'E' network IP address), username and password. If the authentication was successful, external users would receive 'D' network IP address and could access internal resources. Unauthorized zone's users could connect to VPN Server via 'C' network. After authentication, the unauthorized zone's users would receive 'D' network IP address as well. Thus, two groups of users could access the internal network simultaneously.

4. Performance Evaluation

We have implemented this system and tested it in order to make sure that it could be used properly. Moreover, its performance was evaluated. The three performance issues consisting of the security, speed, and cost were studied.

4.1. Security

We have tested this model with several attacking techniques, such as MAC spoofing, IP spoofing, and top 10 attacking techniques ranked in the OWASP[9] web-site. The results are shown in Table 1.

Table 1. The results from using an attacking test.

Technique	**Result**
Setting MAC address as an authenticated user's MAC	Cannot be hacked
Setting IP address as an authenticated user's IP	Cannot be hacked
Setting both MAC and IP address as an authenticated user's MAC and IP	Cannot be hacked
Setting IP address as the internal network's IP	Cannot be hacked
Sniffing data and passwords	Cannot be hacked
Sniffing Cookie/Session ID and attacking by using Session Hijacking	Cannot be hacked
Attacking VPN server by using SQL Injection	Cannot be hacked
Attacking VPN server by using XSS and CSRF	Cannot be hacked
Sniffing users' password when they log in VPN server	Cannot be hacked
Sniffing Session ID sent between users and VPN server	Cannot be hacked

4.2. Speed

The speed of our reverse VPN system was evaluated and compared with a normal network (not using VPN). The results are shown in Tables 2. We measure responding times when users request the top-10 world's popular web-sites.

Table 2. The results of the response times

Target	HTTP response (sec)	
(Ranked by popularity)	Not VPN	VPN
www.google.com	9.38	14.57
www.facebook.com	18.3	21.41
www.youtube.com	9.69	11.28
www.yahoo.com	17.91	24.78
www.blogspot.com	12.47	36.12
www.baidu.com	7.32	11.28
www.live.com	12.68	17.97
www.wikipedia.org	8.43	11.87
www.twitter.com	17.23	28.34
www.qq.com	14.94	-
www.msn.com	13.28	18.36

4.3. Cost

This model used only one computer to work as VPN server while commercial NAC was very expensive (but it can not prevent bypassing authentication with MAC cheating). Obviously, using our model (reverse VPN) could decrease the cost of an implementing secure network.

5. Conclusion

In this research, we searched for a methodology for building NAC that could prevent bypassing authentication with MAC cheating technique. We used 'Reverse VPN' method. The 'Reverse VPN' was the use of VPN in an opposite side. Unauthorized users would connect to VPN server from 'Unauthorized Zone'. If authentication was successful, authorized users would obtain secondary IP address from VPN system. This IP address was in the internal network's IP address groups allowed by firewall to access internet. The authorized users would be able to access resources in the internal network such as printer and shared folder. We have tested this system by testing with MAC spoofing technique and found that this model could prevent this problem. Moreover, we have evaluated this system in three performance issues (security, speed, and cost). We found that our model provided high security. Although VPN may cause a little delay, it is acceptable. However, we can improve the speed by using a high power VPN server. This model has low implement cost compared with a commercial VPN.

6. References

[1] J. Kelley, R. Campagna. *Network Access Control For Dummies*. Denzil Wessels, 2009.

[2] S. McClure, J. Scambray, and G. Kurtz. *HACKING EXPOSED 6 Edition Network Security Secrets & Solutions*. McGraw-Hill Osborne Media, 2009.

[3] *SMAC: MAC-address Changer*., http://www.softpedia.com/get/Network-Tools/Misc-Networking-Tools/SMAC-MAC-Address-Changer.shtml

[4] R. Yuan, W. T. Strayer. *Virtual Private Networks: Technologies and Solutions (1st Edition)*. Addison-Wesley Professional, 2001.

[5] D. Ralph, L. Ted. *The DHCP Handbook: Understanding, Deploying, and Managing Automated Configuration Services*. Pearson Higher Education, 1999.

[6] G. Combs et al. *The Wireshark network protocol analyzer*., http://www.wireshark.org

[7] T.D. Morgan. *Weaning the Web off of Session Cookies*. 2010., http://www.packetstormsecurity.org/papers/web/WeaningTheWebOffOfSessionCookies.pdf

[8] *Session hijacking attack*., http://www.owasp.org/index.php/Session_hijacking_attack

[9] *OWASP Top 10 2007*., http://www.owasp.org/index.php/Top_10_20