# VPN Detection Method using Attacker's Route Information

[1]Dukyun Kim, [2]Byungho Park, *[3]Sungdeok Cha

[1] *Graduate School of Information Security, Korea Univ., Seoul, Korea, kim9069@gmail.com*
[2] *Ministry of National Defense, Seoul, Korea, sunsonbob@naver.com*
[*3] *Dept. of Computer Science, Korea Univ., Seoul, Korea, scha@korea.ac.kr*

Abstract It is very difficult to determine whether VPN or Proxy server exists between Client and Server, or not. Especially, VPN rarely leave network footprints. To solve this problem, this paper analyses VPN connection mechanism and proposes an effective detection method using attacker's routing table.

**Keywords***: VPN Detection, Proxy Detection, Indirect Web Connection*

## 1. Introduction

In most hacking attacks, hackers tend to access target systems in a variety of indirect connection methods in order to hide their own IPs. Particularly, they used VPN in Cyber Attack 320 against Korean broadcasting companies' and banks' sites, and an attack against KHNP.

Most of the security systems depend on rogue VPN IP lists provided by security companies or agencies. Unfortunately, these lists contain only already-known IPs. Although many security experts proposed some useful signatures such as Base64 usage, these metrics are effective only on some proxy servers, not on VPNs [1].

In academic domain, most of the studies have focused on IP Traceback schemes. According to recent survey, however, except for ICMP Traceback, all other traceback schemes require a change in the existing network infrastructure [2]. Moreover, ICMP Traceback is blocked by many network devices worried about DDoS attacks by ICMP flooding.

To overcome these limitations, we analyzed VPN process and extracted some characteristics to determine VPN usage. Based on them, we propose an efficient VPN detection method with high accuracy, and discuss implement issues.

## 2. Analysis of VPN Connection

### 2.1 Normal connection

In case of Normal Connection, Client NIC sends all of Client's traffics to Server NIC without change (see Fig.1).

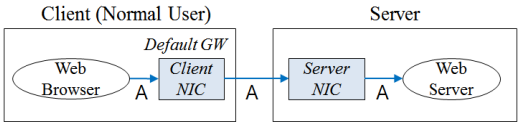


**Figure 1.** Normal Connection Process

In the above diagram, a packet (e.g., GET request) traverses from Web browser to Web server as follows.

① Client NIC receives a packet (type A) from Web browser, as it is the default gateway.

② Client NIC sends the packet (type A) to Server without change (see Table.1).

③ Web Server receives the packet (type A).

**Table 1**. IP Header in case of Normal Conn.

| *Packet Type* | *Source IP* | *Destination IP* |
|---|---|---|
| A | Client IP | Server IP |

### 2.2 VPN Connection

In case of VPN Connection, all of attacker's traffics have to be sent to VPN server to hide attacker's IP. In order to control this distorted flow, most of the VPN tools change Client's network configuration. Firstly, they set up a virtual adapter (i.e., Virtual NIC) in front of the physical adapter (i.e., Client NIC) [3]. Secondly, they assign the Virtual NIC to the default gateway on behalf of the Client NIC.

VPN server receives all traffics generated by Virtual NIC, and connects to Victim computer as if it is a real client (see Fig.2).

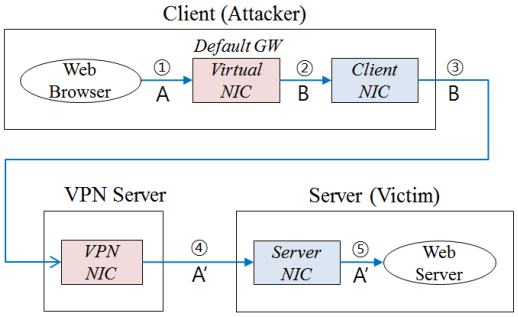


**Figure 2.** VPN Connection Process

In case of VPN connection, a packet traverses from Web browser to Web server via VPN server as follows.

① Virtual NIC receives a packet (type A) from Web browser, as it is the default gateway of Client network.

② Virtual NIC encapsulates the packet (type A), and creates a new packet (type B). After this process, the original packet (type A) becomes a payload of the new packet (type B). VPN server IP is assigned to the destination IP of the new packet (type B) (see Table.2).

③ Client NIC receives the new packet (type B), and sends it to VPN server without change.

④ VPN Server restores the original packet (type A) from the packet (type B). And, it changes the source IP of the restored original packet (type A) from attacker's IP to VPN server IP in order to conceal attacker's origin (see Table.2).

⑤ Web server receives the IP-changed original packet (type A′) in VPN Server. Therefore, he recognizes the VPN Server as his client.

**Table 2**. IP Header in case of VPN Conn.

| ***Packet Type*** | ***Source IP*** | ***Destination IP*** |
|---|---|---|
| A | Virtual NIC IP | Server IP |
| A′ | VPN Server IP | Server IP |
| B | Client IP | VPN Server IP |

# 3. VPN Detection Method

## 3.1 Decision Condition

From the analysis of VPN Connection process, we find two significant differences which can characterize VPN Connection.

First condition is that a Virtual NIC must exit and it performs as the default gateway. However, as many computers use Virtual NIC for various purposes such as packet filtering, this condition alone is possible to cause many false alarms.

Second condition is that a specific route with VPN server IP exists on the attacker's routing table. The role of this route sends all packets heading to VPN server (i.e., type B packets in Fig. 2) to Client NIC. Remember Virtual NIC is the default gateway. So, without this route, operating system will send automatically all of the type B packets to Virtual NIC and may cause endless loop.

The latter is more effective to detect VPN usage than the former. Any normal clients neither generate a packet heading to their own, nor set up a network route for the packet.

## 3.2 Detection Method and Implementation Issues

We propose a VPN detection method based on the above two conditions. As the two conditions exist only in case of VPN connection, our method assures high accuracy.

One limitation of our method is that how to get routing information from clients. Fortunately, it is reasonable that Web server asks for some information to a client in order to protect himself. The most acceptable approach is that Web server sends an open script to suspicious clients and they execute the script by themselves.

Therefore, to implement our method, several studies are required. Firstly, suspicious attackers have to be filtered from normal users as little as possible. Secondly, a VPN detection script needs to operate in various client platforms. At last, the script has to be protected from hacker's attacks.

# 4. Conclusion and Future work

We inspected VPN Connection compared to the Normal Connection. Through the analysis, we find that a Virtual NIC and a specific route with VPN server IP exist whenever an attacker uses VPN. Using two conditions, we propose an effective method to determine VPN connection.

As mentioned above, to implement our method, several future works are required. Above all, we will build a prototype and test it in real field. Furthermore, we will enhance our method to classify VPN type and trace original IP.

# Acknowledgements

This research was supported by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC(Information Technology Research Center) support program (IITP-2015-H8501-15-1012) supervised by the IITP(Institute for Information & communications Technology Promotion).

# References

[1] John Brozycki, "Detecting and Preventing Anonymous Proxy Usage", SANS Institute, 2008.

[2] Vijayalakshmi Murugesan, Mercy Shalinie, and Nithya Neethimani. "A Brief Survey of IP Traceback Methodologies", Acta Polytechnica Hungarica, Vol. 11, No. 9, 2014.

[3] Michael E. Whitman, Herbert J. Mattord, and Andrew Green, "Guide to Firewalls and VPNs", 2011.