# Testing Methods Research and Design for NIPS Anti-evasion Attack

Xuan Li*, Jian Gu and Qian Li
Testing Center, The Third research institute of ministry of public security, Shanghai 200031, China
*Corresponding author

***Abstract*—Based on the test for anti-evasion attack of NIPS, A simple and effective improved software test method is designed. In this improve method testing software are installing and running on physical and virtual machine, the network cards of the virtual maching are set in different operation modes, Software of the test are designed to build the test environment, This improved test method is simplify, saving the testing equipment, the result is correct and effective. Meanwhile, Compared with the test instrumentation Breakingpoint Systems expensive instrument isn't required.**

***Keywords- IPS; evasion attack; testing; breakingpoint systems***

## I. INTRODUCTION

Network Intrusion Prevention Systems (NIDS) has a deep packets inspection capabilities, in depth analysis of various protocols and filtering attacks from packets, could send alarms, linkage or even block response when detected malicious packets, indirectly or directly protect the network. The commonly detection methods of NIPS used are include feature matching, anomaly detection and rule model. Feature matching is deterministic description for known attack or intrusion, to form the corresponding event template, when the NIDS detected events to match the invasion with known patterns, make a response of the alarm and/or blocking. The abnormality detecting method includes statistics of events, statistics of flow and abnormal protocol and so on, formation of a statistical model, commonly used measurement parameters include the number of events, network flow, the protocols out of the common boundary[1-5], when the NIDS detected events statistics, flow or protocol anomaly, make a response of the alarm and /or blocking. Rule model is the use of an expert system with artificial intelligence features, including the knowledge base, inference engine and rules. When NIDS detects the flow break the rules of the rule model, the alarm and/or block is responded. The basic principle of NIPS is in its running, real-time monitoring of network flow, capture packets, and reorganization data packets, and compared with the system database, including baseline, templates, rules models, etc., when the attack is detected, an action is responded.

Aiming to the attack detection method and working principle of NIPS, some attacks are designed and used to evasion detection of NIPS. An improved anti-evasion attack software testing method is designed based on the conventional test method for NIPS anti-evasion attack test method, to consider whether it has functions of certain ability to anti-evasion. The article also through the use of the instrument (BPS Breakingpoint Systems) to simulation evasion attack, test NIPS anti-evasion attack function, and as a reference in experiment.

## II. EVASION ATTACK TECHNIQUES AND TOOLS

### *A. Evasion Attack Techniques*

Evasion attack is to use the new or unconventional techniques and methods to escape or bypass intrusion prevention behavior of NIPS, the evasion techniques involving layer 3-7 of OSI reference model, attacks are rich and methods variety. Mainstream evasion attacks including code modification, session splicing, fragmentation attacks and denial of service attacks, etc. [6-7]. Therefore NIPS need to have evasion detection and attack defenses function, this paper study anti-evasion function testing methods of NIPS.

### *B. Test Tools*

Testing tools can simulate evasion attacks include Blade, Nikto, Fragrouter and other software, use this three software can simulate comprehensive evasion attack packets, and test the ability of anti-evasion of NIPS.

*1) Blade :*Blade is a packets retransmission toolkit for real attacks that allows users to generate pre-defined attack data (.dll files) between two network cards, simulation the system operating in the computer hardware level, simulation of any source IP address and destination IP addresses. Attack operations can be repeated at any time, or according to a pre-defined action occurs. Blade attack library contains more than 600 kinds of pre-recorded attack simulate data, with a dozen evasion attack test pack, including Reverse Backslash, Prepend Random String, Fake Parameter and other distorting attacks and session splicing attacks. To detect the response of NIPS in variety attacks.

*2) Nikto:* Nikto is a Web scan software, it can test variety of security projects of the Web server, can check the HTTP and HTTPS services, while supporting the basic port scan to determine whether the web server is running on other open ports. Nikto may send a large number of requests to the remote host, which may damage the host, remote host and network. Nikto1.35 has nine evasion attack techniques can be used, such as random URL encoding (non-UTF8), use windows directory separator / instead of /, fake parameters to files and session splice technology escape detection of NIPS.

*3) Fragrouter:* Fragrouter is an application with the routing function, it is possible to sent attack flow to victim after the fragmentation process by the attacker, can also intercept, modify and rewrite the packets sent out to achieve a variety NIPS evasion technology, including IP, TCP layer packets fragments and fragments overlap and overflow.

*4) Test Instrumentation:* Breakingpoint Systems is a network security device with attack packets transmission, simulate the online behavior of millions users and many other functions in IXIA company. The device can simulate the network layer, transport layer and application layer and other data flow, and can simulate the TCP, IP fragmentation attacks, which can be used to test anti-evasion attack function of NIPS.

Above software or instrumentation can be conducted evasion attacks test in more comprehensive and complete, in addition to the above software and instrumentation, as well as some software such as Nmap, Snot and ThreatEX equipment also able to launched evasion attack for NIPS, here is not introducted one by one.

## III. TEST ENVIRONMENT AND METHOD DESIGN

### A. *Conventional Test Method*

The network topology of conventional test method is shown in Figure 2.In the case of using the toolkit of software Fragrouter to test fragment evasion attacks, the software Blade is implemented on PC1, and the attacks that can be detected by NIPS are selected. Then, attack packets are transmitted from Subnet 1 through the gateway (PC2) to Subnet 2. The enabled Fragrouter on PC2 will fragment the attack packets, thus fragmented attack packets are broadcasted on Subnet 2. If NIPS is able to detect network attacks, in addition, if the type of each restored attack is consistent with the type of attack originally transmitted by Blade, then it means that NIPS is able to detect fragment evasion attacks; otherwise, fragment attacks of the certain type will not be detected. Since the attack types of Blade are diverse, and an attack packet has its own evasion characteristics, also Fragrouter has multiple means of fragment evasion, thus, a combination of the two software can be exploited to test its ability of detecting evasion attacks [8-12].

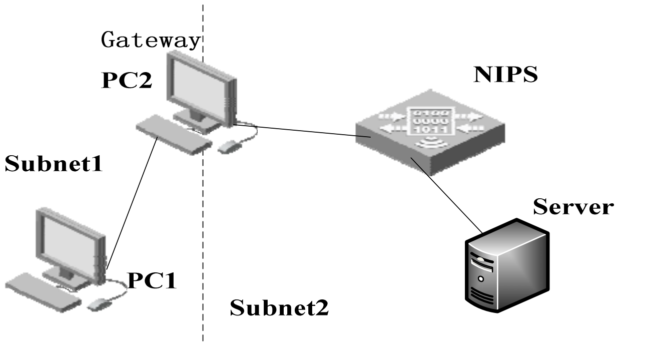


FIGURE I. THE NETWORK TOPOLOGY OF CONVENTIONAL TEST METHOD

When using the toolkit software Nikto to test evasion attacks for Web server, a web site (including dynamic, static web pages and databases, etc.) is built on the server in Subnet 2, and Nikto is enabled on PC2. Random URL encoding evasion attacks are transmitted by the network interface card in Subnet 2 to the web site.If NIPS is able to detect network attacks, additionally, if the type of each restored attack is in accord with the type of attack sent by Nikto, then it means that NIPS is able to detect random URL encoding evasion attacks; otherwise, NIPS does not have such function. Other types of evasion attacks that Nikto transmits can be traversed in test.

### B. *Designed Test Method*

The test method involves two subnet and gateway configuration, test environment to build complex, and not easy to maintain and reuse in 2.1 segment. Designed test method use dual-NIC host to instead of PC1 host and server, use VMware virtual machine running on PC1 replace PC2 that in Figure 2, thereby reduce two physical devices, at the same time virtual machine easy to manage and reuse[13].

*1) Environmental Structures:* The environment of designed test method in this paper shown in Figure 2, using PC host and the virtual machine running on this PC to simulate various evasion attacks.

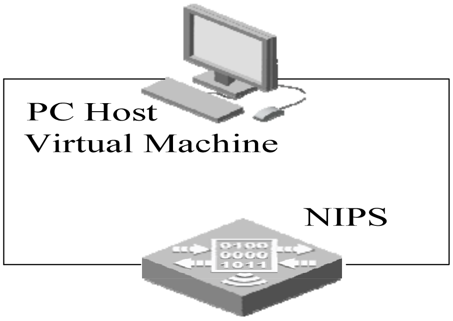


FIGURE II. DESIGNED ANTI-EVASION ATTACK TEST TOPOLOGY

The software installation and setup of the PC host shown in Figure 3, installing Blade, Colasoft, VMware software and set up a Web server on the PC. Use VMware create a Linux virtual machine and add two network cards for it, installing Fragrouter and Nikto software on the virtual machine, a test environment to build complete.

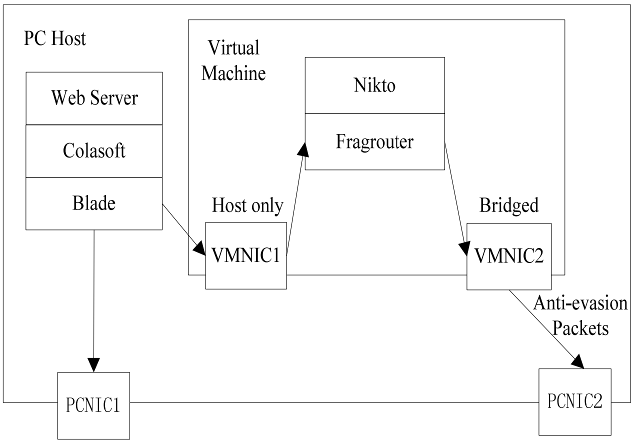


FIGURE III. SETTINGS OF TEST PC

*2) Test Procedure:* This segment provides a brief description of the test method, the test process is described step by step.

Step 1: Configure the virtual machine two NIC's IP addresses and masks, make them in two subnets, such as:

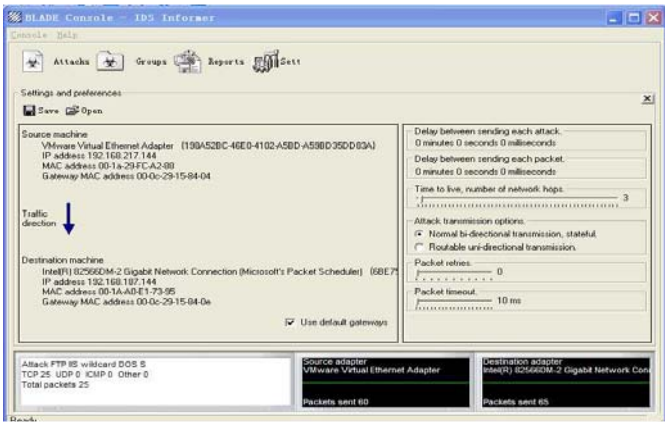
virtual NIC 1: 192.168.217.145/24, virtual NIC 2: 192.168.187.145/24;

Step 2: The NIC1 is set to Host only mode to ensure that the packets through the card is not mapped to the physical NICs, virtual NIC2 is set to Bridged mode, shared physical NIC2 of physical machine;

Step 3: In IDS Informer module of Blade, virtual NIC1 is configured as source machine, IP address is on the same subnet with virtual NIC1, Gateway MAC is set MAC address of virtual NIC1. Physical NIC1 is configured as destination machine of the PC, IP addresses is on the same subnet with physical NIC1, Gateway MAC is set MAC address of physical NIC1, shown in Figure 4;

Step 4: Enable Fragrouter software in the virtual machine, use the command fragrouter -i eth1 -F1, the packets will be fragmented as 8-byte fragmentation IP packets when reach NIC1of the PC;

Step 5: Enable the Wireshark network protocol analyzer tool in the PC, to view the network communication packets between physical NIC1 and the physical NIC2;



Source machine
VMware Virtual Ethernet Adapter (190A52BC-46E0-4102-A5BD-A598D35DD03A)
IP address 192.168.217.144
MAC address 00-1a-29-FC-A2-88
Gateway MAC address 00-0c-29-15-84-04

Traffic direction

Destination machine
Intel(R) 82566DM-2 Gigabit Network Connection (Microsoft's Packet Scheduler) (6BE7
IP address 192.168.187.144
MAC address 00-1A-A0-E1-73-95
Gateway MAC address 00-0c-29-15-84-0e

☑ Use default gateways

Delay between sending each attack
0 minutes 0 seconds 0 milliseconds

Delay between sending each packet
0 minutes 0 seconds 0 milliseconds

Time to live, number of network hops 3

Attack transmission options
● Normal bi-directional transmission, stateful
○ Routable uni-directional transmission

Packet retries 0

Packet timeout 10 ms

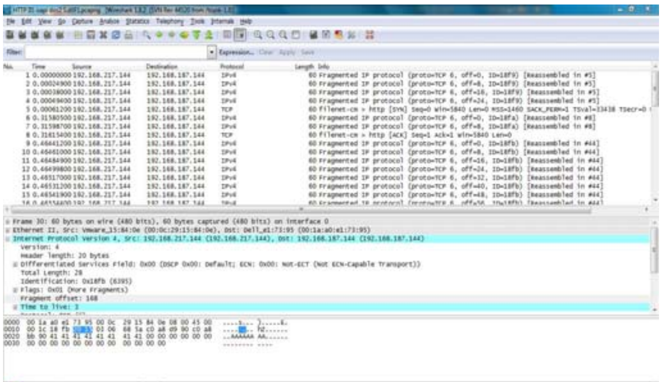
Attack FTP IIS wildcard DOS S
TCP 25 UDP 0 ICMP 0 Other 0
Total packets 25

Source adapter
VMware Virtual Ethernet Adapter
Packets sent 60

Destination adapter
Intel(R) 82566DM-2 Gigabit Network Con
Packets sent 65

FIGURE IV. IDS INFORMER CONFIGURATION

Step 6: Use Blade send attack packets (selected the HTTP IIS isapi dos2 S), view the attack packets of network in Wireshake network protocol analyzer tool's interface, as shown in Figure 5, at the same time to see the response of NIPS whether correct attack is detected.


File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

```
No.  Time        Source           Destination      Protocol  Length Info
  1 0.00000000 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=0, ID=18f9) [Reassembled in #5]
  2 0.00024900 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=8, ID=18f9) [Reassembled in #5]
  3 0.00038000 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=16, ID=18f9) [Reassembled in #5]
  4 0.00049400 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=24, ID=18f9) [Reassembled in #5]
  5 0.00061200 192.168.217.144 192.168.187.144 TCP    60 filenet-cm > http [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK_PERM=1 TSval=13438 TSecr=0
  6 0.31580500 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=0, ID=18fa) [Reassembled in #8]
  7 0.31598700 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=8, ID=18fa) [Reassembled in #8]
  8 0.31615400 192.168.217.144 192.168.187.144 TCP    60 filenet-cm > http [ACK] Seq=1 Ack=1 Win=5840 Len=0
  9 0.46441200 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=0, ID=18fb) [Reassembled in #44]
 10 0.46461000 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=8, ID=18fb) [Reassembled in #44]
 11 0.46484900 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=16, ID=18fb) [Reassembled in #44]
 12 0.46499800 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=24, ID=18fb) [Reassembled in #44]
 13 0.46517000 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=32, ID=18fb) [Reassembled in #44]
 14 0.46531200 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=40, ID=18fb) [Reassembled in #44]
 15 0.46541900 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=48, ID=18fb) [Reassembled in #44]
 16 0.46554400 192.168.217.144 192.168.187.144 IPv4   60 Fragmented IP protocol (proto=TCP 6, off=56, ID=18fb) [Reassembled in #44]

⊞ Frame 30: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
⊞ Ethernet II, Src: Vmware_15:84:0e (00:0c:29:15:84:0e), Dst: Dell_a1:73:95 (00:1a:a0:e1:73:95)
⊟ Internet Protocol Version 4, Src: 192.168.217.144 (192.168.217.144), Dst: 192.168.187.144 (192.168.187.144)
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00: Not-ECT (Not ECN-Capable Transport))
    Total Length: 28
    Identification: 0x18fb (6395)
  ⊞ Flags: 0x01 (More Fragments)
    Fragment offset: 168
  ⊞ Time to live: 3

0000  00 1a a0 e1 73 95 00 0c  29 15 84 0e 08 00 45 00   ....s... ).....E.
0010  00 1c 18 fb 20 15 03 06  68 5a c0 a8 d9 90 c0 a8   .... ... hZ......
0020  bb 90 41 41 41 41 41 41  41 41 00 00 00 00 00 00   ..AAAAAA AA......
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

FIGURE V. NETWORK ATTACK PACKETS ANALYZED OF WIRESHARK

The result analysis of Wireshake showed that the attack packets send form Blade can be fragrouted normally, Formed the fragment packets attack which want to evasion detection, defense from the NIPS, this test method is effective, can be used to test the anti-evasion attack function of NIPS, when testing other ways of evasion and evasion packets can use orthogonal experiment method to traverse other attacks.

The procedures of use Nikto software to test is similar of the above, use virtual machine's NIC2 as the source of the attack in testing, send the attack packets to the physical machine, only need to turn on the Web server built in the physical machine, when the attack occurred, check NIPS whether detect and defense evasion attacks correct.

*3) Background flow:* When test the attacks for the NIPS, usually adding background flow in the attacks flow to simulate real application scenarios. The method use Colasoft package playback software, playback normal network data packets, including TCP and UDP protocols and can adjust the playback speed of the packets, to adjust the proportion of background flow.

### *C. Testing Instrument*

*1) Instrument testing methods:* Breakingpoint Systems instrument can provide standardized, modular attacks, including code modification, fragmentation attacks, and the attacks can be packaged into the module, facilitate to reuse. Make the instrument and NIPS series in a test environment, environment is simple. As shown in Figure 6.

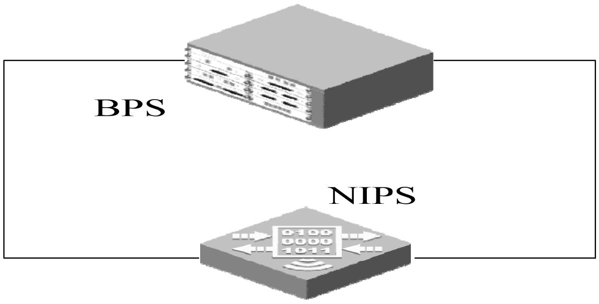
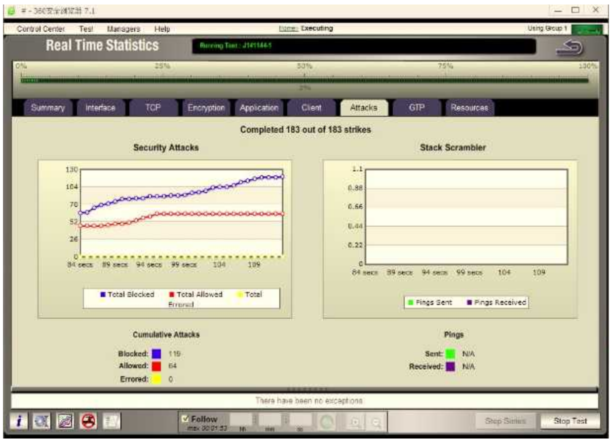


FIGURE VI. BPS TEST ENVIRONMENT TOPOLOGY

Selection the detect module (Security Module) is used when testing, adjust the attack parameters, and select the number of attack packets carry on a evsion attack, the attack process shown in Figure 7, In sending process, view the discovery and defense capability of NIPS, and verify the correctness.

*2) Analysis of test results:* Choosing 183 kinds of different types of attack, and design the evasion methods of attacks, including port redirection, HTTP codes deformation, IP fragmentation, TCP fragmentation. Using the same NIPS separately under the test of instrument testing method, conventional testing method and Improved testing method carried out anti-evasion attack in the benchmark test environment (no background flow), the instrument testing method results as a reference, inspection the evasion attacks identify ability of as well as in the effectiveness of the improved method, the test results shown in Table 1.



Completed 183 out of 183 strikes

Cumulative Attacks

Blocked: 🟦 119<br>
Allowed: 🟥 64<br>
Errored: 🟨 0

Pings

Sent: 🟩 N/A<br>
Received: 🟪 N/A

There have been no exceptions

FIGURE VII. TEST SHOTS OF BPS ATTACK

TABLE I. THREE KINDS OF TEST METHODS COMPARE RESULTS

| | **Instrument testing method(Reference)** | **Conventional testing method** | **Improved test method** |
|---|---|---|---|
| **False positive rate** | 15.73% | 15.73% | 15.73% |
| **False negative rate** | 34.97% | 34.97% | 34.97% |

The false positive rate refers to the percentage of error recognition or reduction the attack methods of NIPS, when test the three kinds of testing methods for 183 species of different evasion attack methods, NIPS detection error in 28 kinds of attacks, and mistake of the attack types are the same. False negative rate is the percentage of can't be detected or reduction the attack methods of NIPS, when test the three kinds of testing methods for 183 species of different evasion attack methods, 64 kinds of attacks can't detected of NIPS, and can't be detected or reduction attack types are the same. From the test results, we can see that the testing method designed in this paper can be used to test the anti-evasion attack ability of NIPS.

## IV. CONCLUSION

Based on the conventional NIPS method, this paper designs a new software testing method, to complete the NIPS anti-evasion attack. Compared with the conventional testing method, this method use the virtual machine to build environment, and it needs to set up the virtual machine NIC and software, environmental build process complex. But which overcomes the conventional software testing environment complex, difficult to maintenance and other shortcomings and use less equipment. at the same time, this paper briefly introduces the instrument test method, the instrument can provide a large number of attack methods and means, which is easy to modify the attack parameters, but requires expensive hardware tools as a test basis, the environment is difficult to achieve. During the experiment to test the results of the instrument as a reference, compared with this paper designed method, the test results are consistent.

## REFERENCES

[1] Olli-Pekka Niemi, Antti Levomäki, Jukka MannerDismantling Intrusion Prevention Systems. ACM SIGCOMM Computer Communication Review, 2012,42(4): 285-286.

[2] George Varghese, J. Andrew Fingerhut, Flavio Bonomi. Detecting Evasion Attacks at High Speeds without Reassembly. ACM SIGCOMM Computer Communication Review,2006,36(4):327-338.

[3] Ye Hui-min,Pan Zheng-yun. IDS Data Collection Mechanism. computer systems applications,2002,11(7):37-39.

[4] XIANG Ga, CAO Yuan-da. Generating IDS Attack Pattern Automatically Based on Attack Tree. Journal of Beijing Institute of Technology, 2003,12(2):138-142.

[5] ZHANG Yan-jun, JIA Shi-guo, XUE Xiao-min. Detection of intrusion and attack from SYN Flood with Ipv6. Journal of Lanzhou University of Technology, 2008,34(2),104-107.

[6] Zhou Yang. Application of Protocol Analysis Technology in IDS. computer systems applications, 2011,20(6):161-164.

[7] Lu Zhen,Gu Jian. Application of orthogonal test method in IDS test. Information network security,2010.02,24.

[8] Wu Yin,Ye Xin-ming,Gong Han-ming. Research on the method of combining IDS active testing and passive testing. Journal of Inner Mongolia University, 2013,44(1):97-103.

[9] Zhou Chun-ming,Yang Shu-tang. Research on IDS anti-evasion technology for IP slicingComputer applications and software,2007,24(10):22-25.

[10] Huang Lu,Yu Hong-jie. Enhancing counting bloom filters through Huffman-coded multilayer structures, IEEE/ACM Transactions on Networking (TON),2010,18(6):1977-1987.

[11] Xia Qin,Wang Zhi wen, Lu Ke. The method of using information entropy to detect network attacks in Intrusion Detection System. Journal of Xi'an Jiaotong University, 2013,47(2):14-19.

[12] LIU Lin-qiang, SONG Ru-shun, XU Feng .Study and design of intrusion defense-in-depth system. Computer Engineering and Design. 2005,26 (6):1522-1526.

[13] Li Xuan,Li Yi,Chen Yan. Testing Methods for IDS Anti-Evasion Attack. computer systems applications,2014,23(10):202-206.