The Firewall Rule Authentication Method Based on 6to4 Tunnel

Li Zhou[1], Liangyi Gong[2] and Xin Zou[1]

[1]National Computer network Emergency Response technical Team/Coordination Center of China
[2]Harbin Engineering University, P.R.China
gongliangyi@hrbeu.edu.cn[2]

Abstract

The enterprise internal information security faced with many hidden trouble, and information leakage has been the largest security problem. Firewall is the main technology to solve information leakage, but end-to-end cryptograph tunnel communication can through firewall information filtering detection. In order to prevent the information leakage, it is common to add the block rules in firewall. There is short of a simple and effective verification method for the correctness of firewall blocking rules. We raise a method to verify firewall rules based on dual-protocol. With 64 tunnel technology, virtual an external node, analog communication scene between inside and outside, to verify the effectiveness of firewall rules. The experiments shows that this method is simple to deploy, and can verify rules effectively.

Keywords: *information leakage, firewall rules, validation, dual protocol*

1. Introduction

At present, many modern high-tech enterprises which the information construction is more developed, are facing internal information leakage issues [1]. According to the investigation of Shenzhen Sinfors Technology Co. Ltd in 2006, the Internet information leakage event during working, whose 9% through the BBS and personal blog, 14% through FTP and other file transfer method, 22% through client or Web email, 31% are sent to friends via chat. In order to protect the confidentiality of internal information leakage for intentional or accidental, a technique have emerged which called DLP (the Data leakage prevention),also known as ILP (Information leakage prevention) [2]. DLP is an application technology which through a technology or management tools to prevent specific data or information assets within the enterprise from leaking [3].

Currently, information leakage defense can be divided into two main categories: one is the active protection that protect data by data encryption, information block filtering technology; Another is passive protection, through access controlling and output controlling technology to protect data [4].

According to the enterprise's security policy, firewall maintains an access control list to determine the actions that should take when a packet arrives. The access control list is made up of many list items, each item in the list is called a rule, each rule in turn is made up of 3 parts: rule number, filtering domain and action domain. Rule number is the order of rules in the access control list, ensure that the packet matches the order. Filter domains can be formed from many items, but commonly used are 5: source IP address, destination IP address, source port, destination port, and Protocol. Action domains typically have only two choices: accept, packet is allowed pass through the firewall; refusal, not to allow packets to pass through [5]. Firewall not only prevents undesirable traffic from accessing the internal network, it can prevent a specific communication from the internal network. You can set up a firewall to block certain types of outgoing Protocol, such as the protocol used by P2P software, SSL protocol, IPsec protocol, and so on.

The growing of networks and Web applications makes the security policy of the firewall be more and more complex. Rules in firewall policy set is increasing, plus there is many factors such as the inevitable human error when editing a rule, almost all sets of rules will exist more or less errors and redundant [6], thus the planed security policies cannot be effectively implemented. Currently the authentication methods of rule set are cumbersome, particularly end-to-end protocol which needs to deploy test node in internal and external network, but it is difficult to deploy test node in external network. With the continuous development of IPv6 network, many modern enterprises are deploying IPv6 networks, in order to enhance the information supervision in the IPv6 network, security gateway firewall rules need to be verified. This article for the current transitional phase of enterprise internal information leakage issues, proposed a lightweight security gateway firewall rules verification method based on dual protocol, the method is simple, can effectively improve the efficiency of validation.

2. Attack for Internal Information Leakage

Currently, in order to prevent information leakage, many company deployed security gateways to filter and detect the access to the company network data. But the attacker of internal attack in network information systems is its users and designers, there are many differences from external attack, simple from the angle of technology, cannot comprehensive the truth of internal attack, constitute internal attack will at least needs three factors: people (internal personnel), tool and environment, but must carry out research on human [7].

Paper [7] proposes the integrated model of internal attacks, as shown in Figure 1. Which define the necessary factors, human, tools, and environments; observable information network systems such as databases, network topology, firewall and the configure of intrusion detection system, system vulnerability etc; specific internal attacks: theft of information, set the "logic bombs", or virus, or leave secret passageways in the safety facilities. The output part of the Internal attack integrated model is the consequences of the attack: the confidential file leakage, destruction of normal business in the financial system, the company almost paralyzed.

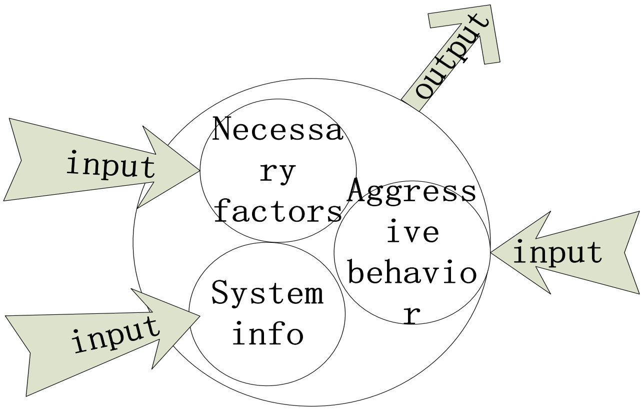


Figure 1. Integrated model of internal attacks

At present most of the security gateway is based on plaintext, bad employees to avoid detection of corporate security gateways, privately establish tunnel with the external to transfer data and disclose the company's confidential information. For example Figure 2, node B access the external network in plaintext, but because of the firewall, it will be cut off from its internal data which contains confidential information, but user A with external network user M establish a secret tunnel, dodging the firewall rules, leak company internal confidential information to external networks.

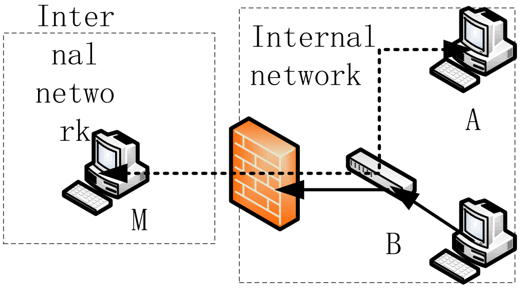


Figure 2. Internal information leakage

Assuming the internal network node collection I, the external network node collection O, $\forall A \in I$, $\exists M \in O$ Let A and M can be interconnected through a secret tunnel.

Discriminant function $P(A, M) = \begin{cases} 1 & KEY(A, M) = 1 \\ 0 & KEY(A, M) = 0 \end{cases}$

As shown in Figure 3:

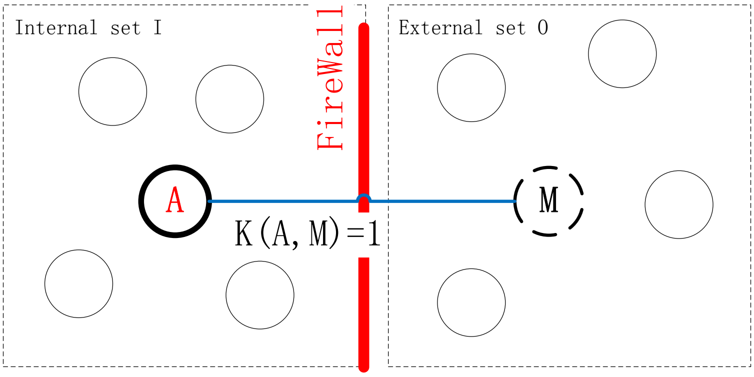


Figure 3. Leakage attacks model

3. Validation Algorithm

In order to prevent internal information leakage, many companies configure redaction protocol rules in the secure gateway to block secret tunnel between external and internal computer network. Current, lack authentication method to configuration rule, because cipher tunnel is end-to-end connection, if you need to detect the enable of rules, you need to deploy test node in external network. But deployment node in external network is difficult, administrators cannot be deploy node in external network.

This article proposes a authentication algorithm based on dual-protocol. The algorithm does not require deploying testing node in external network to take end-to-end redacted communications to verify the firewall rules. Administrator can operate in the internal corporate network, it is convenient and efficient.

Authentication algorithm consists of two parts, the first part is to verify that servers can connect each other, the second is to verify that the configuration of firewall gateway takes effect. The specific algorithm process:

A. verifying the correctness of server interoperability

1) a,b created in the IPv4 network nodes, configure an IPv4 address;

2) seeking external 64 tunnel proxy, apply for IPv6 address for a and b to the outside tunnel proxy;

3) nodes a and b establish connections with 64 tunnel proxy gateway, virtual external node A,B;

4) a and b communicate using the IPv6 address;

5) if the communication success, then the configuration is correct on both ends or fails.

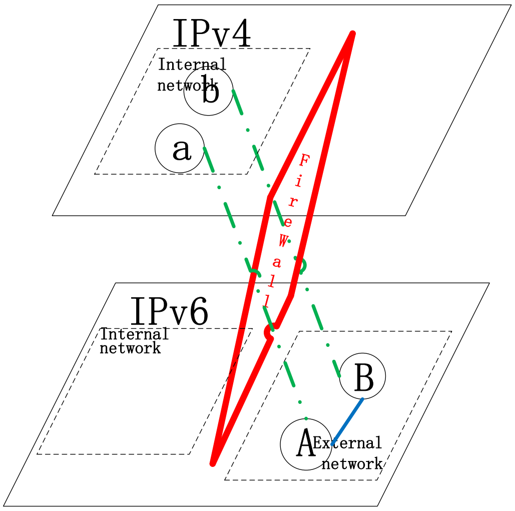


Figure 4. Server interoperability verification model

B. verifying the gateway firewall rules

1) creates a node b in the IPv4 network, configure an IPv4 address;

2) look for an external 64 tunnel-agent, b apply for IPv6 address to external 64 network tunnel proxy;

3) node b connect to 64 tunneling gateway, virtual external networks node b;

4) created node a in the IPv6 network , configure a IPv6 address , and then a establish a connection to b;

5) If a and b can communicate, then firewall blocking rule is not taking effect, or success.

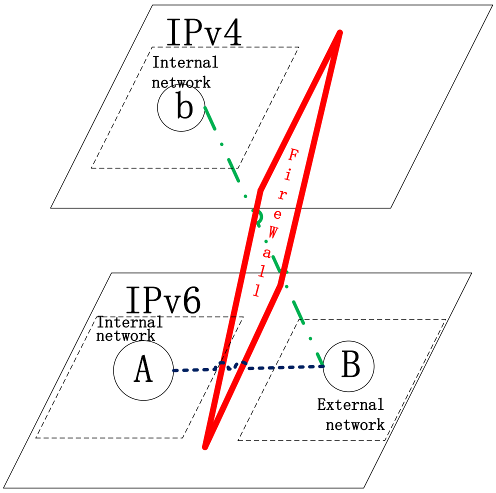


Figure 5. The network model based on dual-protocol security rules

4. Experimental Design and Analysis

IPsec tunneling is widely used in cipher text tunnel. In the firewall rule, add rules to block the IPsec protocol for experimental, preventing internal staff and external network node communicate via Ipsec and create secret tunnel.

A complete IPsec communication consists of two phases, first the IKE negotiation process, negotiate encryption and authentication algorithms, and establish an encrypted channel, and communicate in the channel of (ESP/AH).

IPSec process analysis:

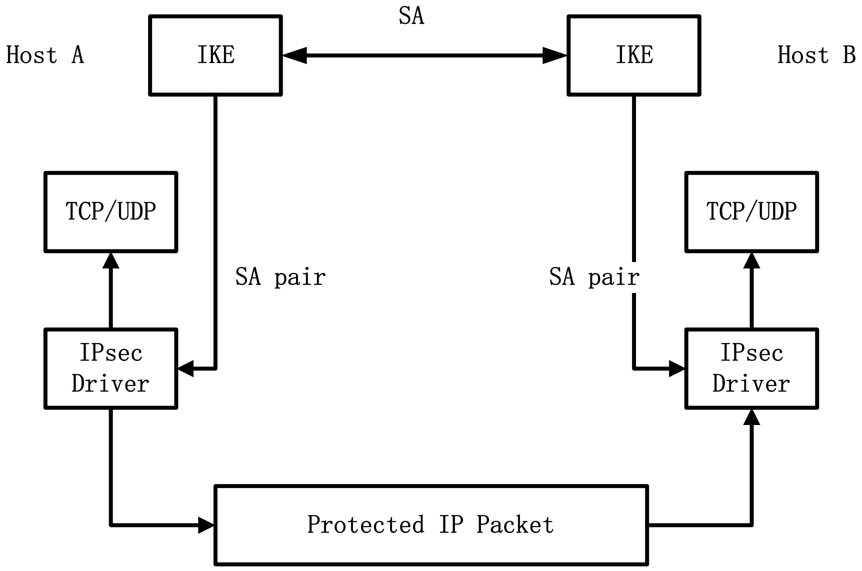


Figure 6. IPsec negotiation process

A) user A (on the host a) sent a message to a user B(host b);

B) IPSec driver checks IP filter on host A to see if packets need to be protected and needs what kind of protection;

C) drivers notify IKE begin security consultations;

D) IKE request is received at host B;

E) SA established the first stage between two hosts, each generates a shared "master key". If two machines has establish the first stage of SA, it can go directly to the second stage consultations;

F) negotiate the second phase of SA: inbound and outbound SA. SA includes SPI, destination IP, key, algorithm, session key etc;

G) IPSec driver on host A uses the outbound SA to sign the packet (integrity checked) and/or encryption;

H) driver transmit the packet to IP layer, and then the IP layer forwards the packet to host B;

I) the network adapter driver on host b receives the packets and pass them to the IPSec driver;

J) the IPSec driver on host b uses the inbound SA checks the integrity signature and/or decrypt the packet; driver decrypted the data package and submit to the upper-layer TCP/IP driver, then the TCP/IP driver submit to host B;

So verifying firewall rules needs to verify the validity of two parts: first, IKE negotiation blocking certification; Second, IPsec cipher text communications block validation. Experimental environment is RedHat operating system, based on the 2.6.18 kernel, using strongswan4.5 to IKE negotiation, use X.509 Protocol to issue digital signature certificates in two copies.

4.1 6to4 tunneling and 6to4 tunneling IPsec communications

Two internal network computer configured with the IPv4 address each establish a tunnel with the external network IPv6 Tunnel Broker, two computers through the tunnel to establish IPsec connections. Because IPv6 packets are encapsulated in IPv4 packets, firewall rules only block IKE negotiation and ESP/AH agreements in IPv6 protocol, so the two nodes can take normal consultation and communication. The experimental procedures are as follows:

1) Experimental network topologies.

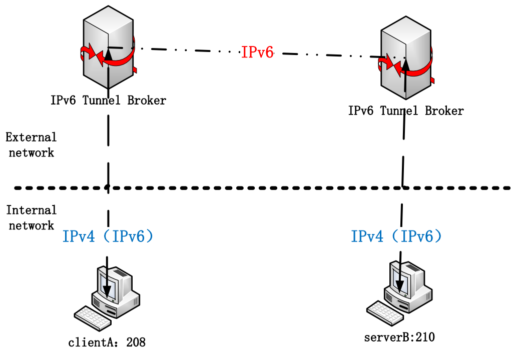
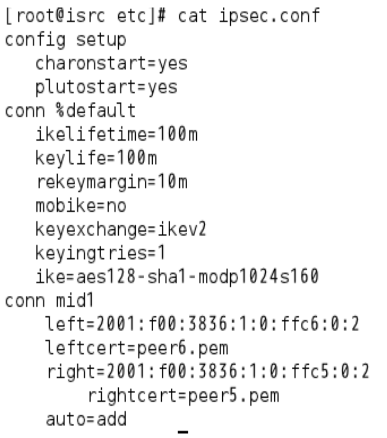


Figure 7. Establish IPsec connections topologies

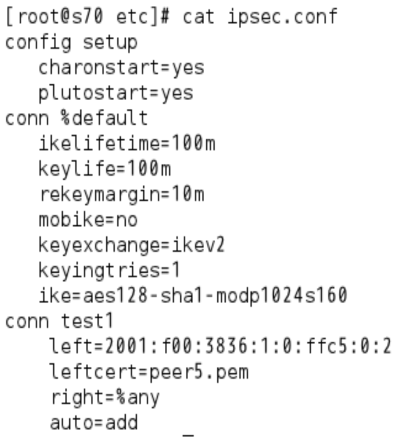
After client A establishes the tunnel, tunnel agent assigns a globally unique IPv6 address to A: 2001:f00:3836:1:0:ffc6:0:2, after server-side B establish the tunnel, tunnel agent assigns B a globally unique IPv6 addresses: 2001:f00:3836:1:0:ffc5:0:2.

2) Configuration of IKE negotiation rule.



```
[root@isrc etc]# cat ipsec.conf
config setup
   charonstart=yes
   plutostart=yes
conn %default
   ikelifetime=100m
   keylife=100m
   rekeymargin=10m
   mobike=no
   keyexchange=ikev2
   keyingtries=1
   ike=aes128-sha1-modp1024s160
conn mid1
    left=2001:f00:3836:1:0:ffc6:0:2
    leftcert=peer6.pem
    right=2001:f00:3836:1:0:ffc5:0:2
        rightcert=peer5.pem
    auto=add
```

Figure 8. The client A's IPSec configuration



```
[root@s70 etc]# cat ipsec.conf
config setup
   charonstart=yes
   plutostart=yes
conn %default
   ikelifetime=100m
   keylife=100m
   rekeymargin=10m
   mobike=no
   keyexchange=ikev2
   keyingtries=1
   ike=aes128-sha1-modp1024s160
conn test1
    left=2001:f00:3836:1:0:ffc5:0:2
    leftcert=peer5.pem
    right=%any
    auto=add
```

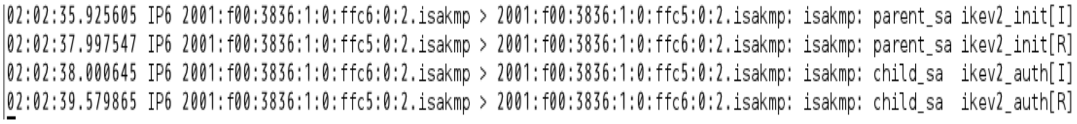
Figure 9. The server B's IPSec configuration

On the client, set the IKE negotiation protocol IKEv2, negotiate encryption and authentication algorithms aes128-SHA1-modp1024s160 in the strongswan's configuration and the other parameters configuration instructions you can follow official description of the strongSwan. Source IP is 2001:....:ffc6:0:2, the certificate is peer6.pem, the server IP is

2001:...:ffc5:0:2, and certificate is peer5.pem. On the server side, exchange protocal and algorithms is the same with the client, local IP is 2001:..:ffc5:0:2 and local server-side certificate is peer5.PEM,listening any exchange requests from the client.

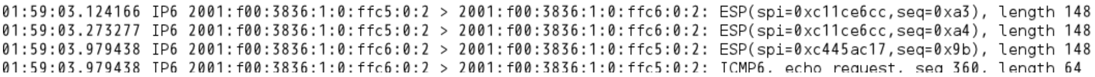
3) Tunnel consultations and Redaction communication.

In the IKEv2 Protocol, consultation was divided into two phases, the first phase is called the initial phase, the second phase is called CREATE_CHILD_SA Exchange, respectively, these two phases consulate IKE SA and CHILD SA. Upon completion of the first phase, a certified secure channel is established between the two sides, the IKE SA. And then under the protection of the secure channel, negotiate SA for IPsec security services, CHILD SA.



```
02:02:35.925605 IP6 2001:f00:3836:1:0:ffc6:0:2.isakmp > 2001:f00:3836:1:0:ffc5:0:2.isakmp: isakmp: parent_sa ikev2_init[I]
02:02:37.997547 IP6 2001:f00:3836:1:0:ffc5:0:2.isakmp > 2001:f00:3836:1:0:ffc6:0:2.isakmp: isakmp: parent_sa ikev2_init[R]
02:02:38.000645 IP6 2001:f00:3836:1:0:ffc6:0:2.isakmp > 2001:f00:3836:1:0:ffc5:0:2.isakmp: isakmp: child_sa  ikev2_auth[I]
02:02:39.579865 IP6 2001:f00:3836:1:0:ffc5:0:2.isakmp > 2001:f00:3836:1:0:ffc6:0:2.isakmp: isakmp: child_sa  ikev2_auth[R]
```

Figure 10. Client A and server B consult over the IKEv2 Protocol



```
01:59:03.124166 IP6 2001:f00:3836:1:0:ffc5:0:2 > 2001:f00:3836:1:0:ffc6:0:2: ESP(spi=0xc11ce6cc,seq=0xa3), length 148
01:59:03.273277 IP6 2001:f00:3836:1:0:ffc5:0:2 > 2001:f00:3836:1:0:ffc6:0:2: ESP(spi=0xc11ce6cc,seq=0xa4), length 148
01:59:03.979438 IP6 2001:f00:3836:1:0:ffc6:0:2 > 2001:f00:3836:1:0:ffc5:0:2: ESP(spi=0xc445ac17,seq=0x9b), length 148
01:59:03.979438 IP6 2001:f00:3836:1:0:ffc6:0:2 > 2001:f00:3836:1:0:ffc5:0:2: ICMP6, echo request, seq 360, length 64
```

Figure 11. Both ends in ESP tunnel mode

4) Analysis of the conclusions.

Judging from the above experiment, two machines through the 6to4 tunnel successfully completed the IKEv2 negotiation process, establish IPsec encrypted channels, and complete the redaction of data transmission under the ESP protocol. So two end-to-end servers can take IPsec negotiation in external IPv6 environment and communicate.

4.2 IPv6 communicate with 6to4 under IPsec tunneling

A machine in the internal network configured a globally unique IPv6 addresses, another machine connect with IPv6 Tunnel Broker in the external network, assigned a globally unique IPv6 addresses by a tunnel agent. Because the gateway in the company issues IPv6 IPsec firewall control rules, so IPv6 client in internal network is unable to communicate with IPv6 Broker in external network directly, the success of IKE negotiation process is dependent on the gateway regulatory policies (based on port or flow feature). Specific laboratory procedures are as follows:

1) Experimental network topologies.

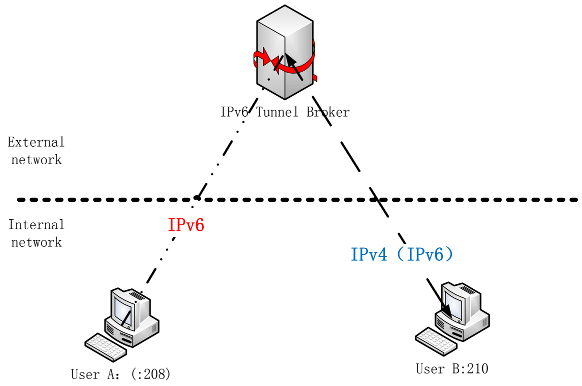
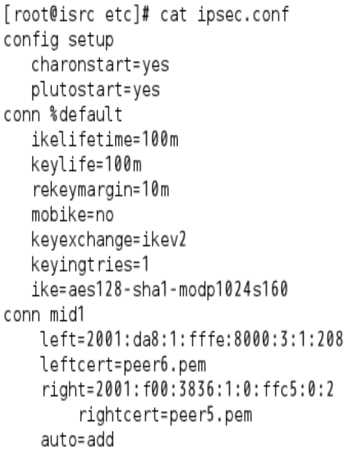


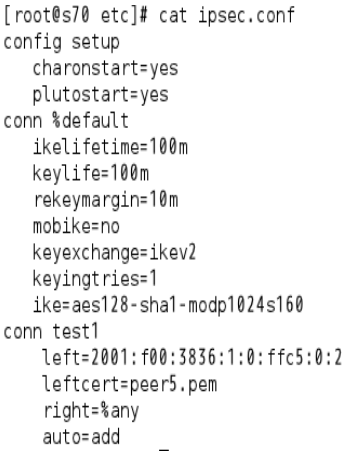
Figure 12. Experiments II network topology

2) IKE negotiation rule configuration.



```
[root@isrc etc]# cat ipsec.conf
config setup
   charonstart=yes
   plutostart=yes
conn %default
   ikelifetime=100m
   keylife=100m
   rekeymargin=10m
   mobike=no
   keyexchange=ikev2
   keyingtries=1
   ike=aes128-sha1-modp1024s160
conn mid1
    left=2001:da8:1:fffe:8000:3:1:208
    leftcert=peer6.pem
    right=2001:f00:3836:1:0:ffc5:0:2
        rightcert=peer5.pem
    auto=add
```

Figure 13. The client configuration

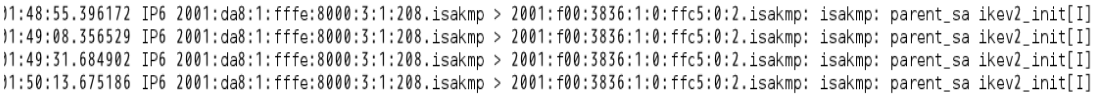


```
[root@s70 etc]# cat ipsec.conf
config setup
   charonstart=yes
   plutostart=yes
conn %default
   ikelifetime=100m
   keylife=100m
   rekeymargin=10m
   mobike=no
   keyexchange=ikev2
   keyingtries=1
   ike=aes128-sha1-modp1024s160
conn test1
    left=2001:f00:3836:1:0:ffc5:0:2
    leftcert=peer5.pem
    right=%any
    auto=add
```

Figure 14. The server configuration

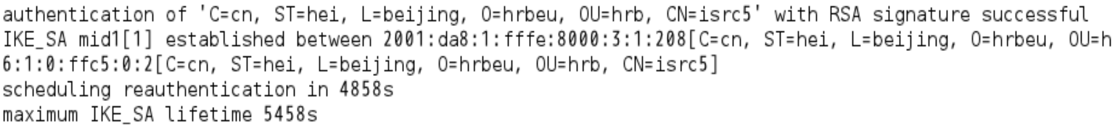
Client is assigned a globally unique IPv6 addresses: 2001:DA8:1:FFFE:8000:3:1:208, after server-side B establish the tunnel, tunnel agent assign B a globally unique IPv6 addresses: 2001:f00:3836:1:0:ffc5:0:2. In the client configuration file, specify the source IP and destination IP, as well as client-side and server-side certificate. The server side specify the source IP and use server-side certificate, listens on any connection request on the right side. After the client start IPsec (#IPSec start), run IPSec up mid1, IKE negotiation requests is initiated to the server side.

3) Tunnel consultations and Redaction communication.



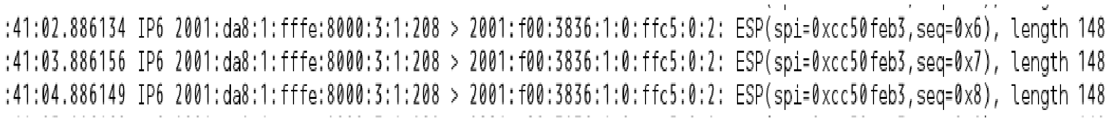
```
1:48:55.396172 IP6 2001:da8:1:fffe:8000:3:1:208.isakmp > 2001:f00:3836:1:0:ffc5:0:2.isakmp: isakmp: parent_sa ikev2_init[I]
1:49:08.356529 IP6 2001:da8:1:fffe:8000:3:1:208.isakmp > 2001:f00:3836:1:0:ffc5:0:2.isakmp: isakmp: parent_sa ikev2_init[I]
1:49:31.684902 IP6 2001:da8:1:fffe:8000:3:1:208.isakmp > 2001:f00:3836:1:0:ffc5:0:2.isakmp: isakmp: parent_sa ikev2_init[I]
1:50:13.675186 IP6 2001:da8:1:fffe:8000:3:1:208.isakmp > 2001:f00:3836:1:0:ffc5:0:2.isakmp: isakmp: parent_sa ikev2_init[I]
```

Figure 15. The client IKE initiate negotiation for the port 500 connection, no server-side response data



```
authentication of 'C=cn, ST=hei, L=beijing, O=hrbeu, OU=hrb, CN=isrc5' with RSA signature successful
IKE_SA mid1[1] established between 2001:da8:1:fffe:8000:3:1:208[C=cn, ST=hei, L=beijing, O=hrbeu, OU=h
6:1:0:ffc5:0:2[C=cn, ST=hei, L=beijing, O=hrbeu, OU=hrb, CN=isrc5]
scheduling reauthentication in 4858s
maximum IKE_SA lifetime 5458s
```

Figure 16. 45500 port IKE negotiation request success



```
:41:02.886134 IP6 2001:da8:1:fffe:8000:3:1:208 > 2001:f00:3836:1:0:ffc5:0:2: ESP(spi=0xcc50feb3,seq=0x6), length 148
:41:03.886156 IP6 2001:da8:1:fffe:8000:3:1:208 > 2001:f00:3836:1:0:ffc5:0:2: ESP(spi=0xcc50feb3,seq=0x7), length 148
:41:04.886149 IP6 2001:da8:1:fffe:8000:3:1:208 > 2001:f00:3836:1:0:ffc5:0:2: ESP(spi=0xcc50feb3,seq=0x8), length 148
```

Figure 17. Consultations after the success of ESP encrypted transmission, no server-side reply packet

4) Analysis of the conclusions.

Judging from the above experiment, if the client IKE negotiation port is 500, then it is unable to complete normal IKE negotiation; and if transmission of IKE negotiation port is 45,500, it can complete the IKE negotiation; but even complete the normal consultation connection, the client may issue a ciphertext packet, but the server-side is still not receiving the ESP or AH packet. Then the firewall can barrier 500 port IKE negotiation packets and packet ESP/AH, but was unable to barrier private modified port of the IKE negotiation packets. Verified the gateway firewall configuration of IPv6 IPsec policy is in effect can prevents ESP/AH under the IPsec protocol communication and prevents company internal information from leakage.

5. Conclusions

As the enterprise network security barrier, the firewall plays an important role. However, if you do not configure the firewall properly, this barrier is useless. Current the study of firewall rules configuration validation are not too much, the IPsec firewall rule authentication method based on the 6to4 tunnel mode proposed in this article is simple and practical, can be applied to verify that the IPv6 network environment inside and outside end to end communications policy effectiveness, research and experiments can be taken on the method used for other firewall rules based correctness verification in the future. The experiment validate that firewall rules can block IPsec communications but also exposed the lack of 6to4 tunnel under the redaction of the firewall traffic monitoring, result in leakage of internal information to network.

References

[1] T. Li, "Protection against leakage of internal information technology', University of Electronic Science and Technology of China, TP309.08, **(2009)**.

[2] Z. Tang, Z. Tian and B. Wang, "Design and implementation of network intrusion detection system", Beijing, Publishing House of Electronics Industry, **(2002)**.

[3] Y. Zhong, "Principles of Information Science, Third Edition", Beijing, Beijing University of posts and telecommunications Publishing House, **(2002)**.

[4] X. Zhang and Q. Tian, "New Methods to prevent Information Leakage", Computer World, **(2009)**.

[5] W. Wang, W. Chen, W. Zhu and H. Chen, "Algorithm for detecting firewall rule configuration quickly", Computer Engineering, **(2007)**.

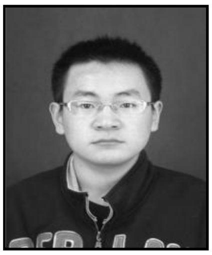
[6] A. Wool, "A Quantitative Study of FirewaIl Connguration Errors", Proceedings of IEEE Computer, IEEE Press, **(2004)**.

[7] K. Lan, F. Yong, A. Zhou and Y. Li, "Network Information System insider threat model", Computer Engineering and Applications, **(2004)**.

Authors

Xin Zou received the Master degree from the Department of Science and Technology from Harbin Institute of Technology, China in 2003. Since 2008, he has worked in National Computer Network & Information Security Administrative Center. He current research interests mainly include routing protocol and algorithm design, performance evaluation and optimization for networks.

Zhou Li received the Master degree in Electronic and Information Engineering from Harbin Institute of Technology in 2005, and received Ph.D. from Beihang University in 2011. Her research interests include information security and avionics network, email: zhouli@cert.org.cn.



Gong Liangyi born in 1987, now is the PhD student of the Computer Science and Technology Department of the Harbin Engineering University. His research interests include information security and wireless sensor network security email: gongliangyi@hrbeu.edu.cn.