Research on high security of IP tunnel in virtual private network

Weimin Gan¹*, Xiaogui Yin²

¹ Department of network technology, Software engineering Institute of Guangzhou, Guangzhou, Guangdong Province, 510990, China
² Department of teaching guarantee, Software engineering Institute of Guangzhou, Guangzhou, Guangdong Province, 510990, China
*Corresponding author’s e-mail: gwm@sise.com.cn

Abstract. IPSec encrypts and authenticates the packets of IP protocol. Both sides of IP network layer communication use encryption authentication, data source authentication and integrity verification to ensure the integrity, confidentiality and anti replay of IP protocol packet transmission. In enterprise network management, we can usually use IPSec VPN technology to establish a secure channel to realize the secure communication between headquarters and branches.[1]

1. Introduction
The old TCP/IP network is lack of security authentication and secrecy mechanism. With the expansion of the scale of enterprise network development and the increasing importance of network security technology, the problem of security policy is becoming more and more necessary, and the introduction of IPSec Security policy is becoming more and more important to ensure the security of the traditional TCP/IP protocol network data communication, the sender can encrypt the data in the form of ciphertext, and the receiver can verify the data to ensure that the data packets are not tampered in the transmission process. Using a good security strategy can not only ensure the security of the communication data, but also prevent the unknown users from sending the captured data packets repeatedly a malicious attack.

2. Application scenarios
In enterprise network management, network administrators usually use IPSec VPN technology to ensure the security of some private data in the public network transmission, and ensure the confidentiality and integrity of data. Administrators often set up IPSec tunnels between the edge routers of enterprise headquarters and branch routers, deploy IPSec VPN technology solutions, and realize network security transmission of data traffic from designated departments. [2]

3. IPSec architecture
IPSec mainly includes three protocols: AH (authentication header), ESP (encapsulating security payload) and IKE (Internet Key Exchange). AH protocol is mainly used for data source verification, data integrity verification, anti message replay and other functions. ESP protocol is mainly used to encrypt ip message data, in this way, ip data packets can be transmitted in a secure network. IKE protocol is mainly used for automatic negotiation of cryptographic algorithms used by ah and ESP, establishment and maintenance of SA and other services
4. IPSec encapsulation mode[3]

There are two encapsulation modes of IPSec protocol: Transport and Tunnel.

4.1. In transmission mode, AH or ESP header is located between IP header and TCP header. Before and after AH and ESP processing, the IP header remains unchanged, which is mainly used in end to end application scenarios. That is, it can only be suitable for PC to PC scenarios, style and spacing.

| AH | ESP |
|----|-----|
| IP Header | AH header | TCP Header | data |
| authentication part |

4.2. In tunnel mode, IPSec will generate a new IP header in front of AH or ESP header. After AH and ESP processing, an external IP header is encapsulated, which is mainly used for site-to-site application scenarios. It can also be applied to any scenario. As tunnel mode requires more IP header overhead, it is recommended to use transmission mode in PC to PC scenario.

| AH | ESP |
|----|-----|
| New IP Header | AH Header | IP Header | TCP Header | data |
| authentication part |

5. Security policy design process

5.1. Configure network accessibility

Check the network layer accessibility between the sender and the receiver to ensure that the two sides can only carry out IPSec communication by establishing an IPSec VPN tunnel.
5.2. Configure ACL to identify interest stream
Part of the traffic can not meet the requirements of integrity and confidentiality. It is necessary to filter the traffic. Select the interest flow that needs to be processed by IPSec. Different data flows can be defined and distinguished by configuring ACL.

5.3. Create security proposal
In order to transmit data stream normally, IPSec proposes to protect the transmission security of data stream. Both ends of the secure tunnel must use the same authentication algorithm, security protocol, encryption algorithm and encapsulation mode. If you want to establish an IPSec Security tunnel between two security gateways, the IPSec tunnel mode can easily hide the actual source IP and destination IP used in the communication process.

5.4. Create security policy
Each IPSec security policy is identified with a unique name and serial number. The encapsulation mode, security protocol and authentication encryption algorithm defined in the IPSec proposal will be applied in the IPSec policy. IPSec policies can be divided into two types: manual SA establishment and Ike negotiation SA establishment. This paper mainly introduces the strategy of creating SA manually.

5.5. Application security policy
Apply IPSec security policy to an interface.

6. Security policy implementation

- Define ACL flow of interest
  \[\text{[R1-acl-adv-3001]}\]\text{rule 5 permit ip source 10.0.1.0 0.0.0.255 destination 10.0.3.0 0.0.0.255}
  \[\text{[R3-acl-adv-3001]}\]\text{rule 5 permit ip source 10.0.3.0 0.0.0.255 destination 10.0.1.0 0.0.0.255}

- Create security proposal
  \[\text{[R1-ipsec-proposal-tran1]}\]\text{esp authentication-algorithm sha1}
  \[\text{[R1-ipsec-proposal-tran1]}\]\text{esp encryption-algorithm 3des}
  \[\text{[R3-ipsec-proposal-tran1]}\]\text{esp authentication-algorithm sha1}
  \[\text{[R3-ipsec-proposal-tran1]}\]\text{esp encryption-algorithm 3des}

- Creating IP protocol security policy
  \[\text{[R1]}\]ipsec policy P1 10 manual
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]security acl 3001
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]proposal tran1
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]tunnel remote 10.0.23.3
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]tunnel local 10.0.12.1
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]sa spi outbound esp 54321
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]sa spi inbound esp 12345
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]sa string-key outbound esp simple huawei
  \[\text{[R1-ipsec-policy-manual-P1-10]}\]sa string-key inbound esp simple huawei
  \[\text{[R3]}\]ipsec policy P1 10 manual

Figure 1. Experimental topology.
This paper mainly introduces the principle of IPSec protocol, the design and implementation process of application scenario, architecture and security policy of IPSec VPN. It focuses on IPSec proposals, policies and binding methods, defines traffic of interest through ACL application policies, The data flow of interest filtered by IPSec will process and encapsulate the negotiation parameters, and then forward through IPSec tunnel.

References
[1] Tang Xiaomeng, Liu Chang, J. (2016-08) Principle and configuration of IPSec VPN. China cable TV.
[2] Xiao Weiqi, J. (2014-12) Discussion on the application of IPSec VPN Technology in private virtual private network, Information communication.

[3] Wang Da, M. (2017), Huawei VPN learning guide, people's Posts and Telecommunications Press. pp. 30-90.

[4] Dong SHIMENG, Gong maobin, J. (2017-01) Research on VPN network design based on IPSec. Communication management and technology.

[5] Peng Chunyan, Wang Defang, J. (2013-06) Design and Simulation of experimental teaching based on IPSec VPN [J]. Electronic design engineering.