IPSec-VPN Simulation Based on GNS3

Fan Yang [1,a] , Lizhen Zhao [2, b]

[1]School of Computer Science, Zhaoqing University, Zhaoqing, Guangdong, China

[2]Educational Technology and Computer Center Zhaoqing University, Zhaoqing, Guangdong, China

[a]Yangfan9@zqu.edu.cn, [b]sdzlz@zqu.edu.cn

Keywords: IPSec-VPN; GNS3; Network engineering case, Simulation; Network security.

Abstract: For the problem that the practical teaching of network engineering specialty in universities lacks actual network engineering cases, we choose IPSec-VPN as the study object, and based on GNS3 network simulator, we have constructed IPSec-VPN network topology and established a dynamic executable IPSec-VPN network case through the combined application of AH, ESP and IKE Agreement that can simulate a real IPSec-VPN secure network. The operation has simulated the network behaviors with normal communications between sites and analyzed the security of encrypted data packets on the public network, and the test results have verified the correctness and the actual availability of the method.

Introduction

With the development of network technology, the network environment has become more complex, the openness, internationalism and freedom[1] of the network have been more prominent, and the security threats confronted by network also have become more highlighted, which require that the course teaching of network engineering specialty in universities also should focus on the system security in network engineering. However, the current teaching of network engineering specialty is only concerned about the general network technology and principles, IP and VLAN planning, routing & switching, network service construction and other technological contents, it mainly introduces firewalls or packet filtering technology on the aspect of network security and lacks the systematic content of network security design technology, especially the practical teaching can't comprehensively apply the relevant security technologies such as authentication, message encryption and decryption, data integrity verification and secure tunnels due to the lack of real application cases, so it is unable to form an effective control ability for network security, which affects the teaching effects of the specialty seriously. By analyzing the IPSec-VPN-related technologies and protocols and on the basis of in-depth study of GNS3 network simulator[2], this paper has proposed the IPSec-VPN security network design and configuration method based on virtual network environment as well as constructed a site-to-site IPSec-VPN network case based on GNSA that can simulate IPSec-VPN technology design in the real network engineering and also can be widely used in the practical teaching and vocational training of the network engineering specialty in universities with low-cost, flexible, convenient, practical, efficient and other characteristics.

IPSec-VPN technical analysis

IPSec protocol suite

The core technology of IPSec-VPN is IPSec protocol suite mainly including Authentication Header (AH)[3], Encapsulating Security Playload (ESP)[4], Internet Security Association and Key Management Protocol (ISAKMP)[5] and Internet Key Exchange (IKE)[6]. ESP protocol is mainly to provide confidentiality protection and integrity verification to security systems, in which encryption and authentication algorithms are needed; AH protocol is principally to provide integrity verification and it only involves authentication algorithm. Both ESP and AH have passed the corresponding Security Association (SA) negotiated in ISAKMP to describe how to protect communications, which kinds of data streams of communications should be protected and which modes should be used to protect communications, etc. by SA. IKE protocol is to control the process of negotiating SA by ISAKMP, and in order to improve the efficiency of negotiation, IKE divides the process of negotiating SA by ISAKMP into two stages that are respectively IKE SA negotiation and IPSec SA negotiation.

IPSec protocol frame

In order to improve the security and flexibility of IPSec, IPSec has built a framework, mainly including five contents: encapsulation protocol, encapsulation mode, encryption algorithm, hash function and key validity, each content provides a number of options, for example, hash function can select MD5 and SHA-1,etc., encryption algorithm can select DES, 3DES, AES, etc., encapsulation protocol can select AH or ESP, encapsulation mode can select transport mode or tunnel mode, key validity can select 3600S, 1800S, etc. according to actual needs. Thus, users can select the appropriate security algorithms based on their demands, when an algorithm has loopholes, they can not only other algorithms under the item, but also prevent the insecurity of the entire IPSec caused by the security risks, which has provided a flexible setting mechanism of security strategy and formed a normative security strategy after rapid negotiation.

Working principle analysis of IPSec protocol

IPSec protocol defines two databases, in which one is SPD（Security Polity Database）, the other is SAD（Security Association Database）. SAD contains parameter information of each SA, such as AH or ESP algorithm and key, sequence number, protocol mode, as well as SA life cycle. For the processing of outflow data, there will be a SPD data item that contains a pointer pointing to a SAD data item; for the processing of inflow data, it is SAD that will determine how to process data packets. SPD contains various data streams of security strategy information to provide security services to specific data streams, the basis of the classification mainly has source IP address, destination IP address, direction of data flow and high layer protocols and ports, and the rule expression is similar to data packet filtering rules of ACL. SPD sorts different strategies by priority and forms an ordered list of strategies for the data items with different data matching in inflow data and outflow data.

Based on data item rules in SPD for processing IP data packets, according to different security rules of data items, and through IP data packets of IPSec gateway, IPSec protocol has three different security strategies: discarding, processing bypassing IPSee and processing bypassing IPSec. The first strategy doesn’t allow the corresponding IP data packet to pass through the security gateway or to be sent to the upper layer for application; the second strategy allows to send IP data packets unprotected by IPSec protocol; the third strategy requires that the corresponding data packet must

be protected by IPSec protocol and indicate the used security protocols, algorithms and other elements.

IPSec-VPN architecture design

Construction of the network topology

Figure 1 is IPSec-VPN virtual network topology constructed according to the characteristics of IPSec protocol and VPN application scenario, in which the router RA and the switch SW1 are used to simulate one network site LAN1 in VPN application scenario, the router RB and the switch SW2 are used to simulate the other network site LAN2, and R1 and R2 respectively act as IPSec-VPN gateway of the two network sites. In order to effectively simulate the construction of the private security network ability, we select a router as IPSec-VPN gateway to connect both ends of Internet so as to avoid the direct connection of two IPSec-VPN gateways in the simulative topology and keep the complexity of constructing the real IPSec-VPN.

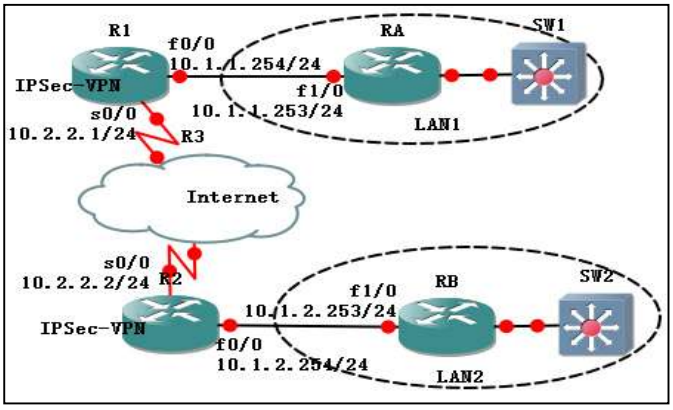

Figure 1 IPSec-VPN simulative network topology

Formulation of the security strategy

An effective IPSec-VPN system should be convenient for network users at the same time of providing the security mechanism that can meet the application requirements, meanwhile, it will not consume too much gateway equipment and resources to avoid the increase of the overlong network delay due to implementation of the security strategy, which requires to find a balance between security and usability. Based on technical principles of IPSec-VPN, the security strategy developed in this case can be divided into two parts; the first part is the security strategy of IKE security tunnel whose main content include (encryption algorithm) with “3DES”, hash algorithm with “MD5“, authentication method with “Pre-Shared Key” and Diffie-Hellman group (DH category) with “group 2 (1024 bit)”. The second part is the security strategy of encryption and integrity verification of data pockets, in which data encryption also uses 3DES algorithm and integrity verification uses ah-sha-hmac.

Configuration of IPSec-VPN

No matter site-to-site IPSec-VPN or remotely accessible IPSec-VPN, the basic configuration process is the same and there are mainly six configuration essentials.

Start using IKE.

Configure the first stage of IKE, including creating ISAKMP strategy and assigning priorities and specifying the symmetric encryption algorithm of plaintext-ciphertext conversion, the hash function for integrity verification of data packets, authentication methods of both sides, DH algorithm level of key exchange, SA life cycle, equipment identification category of IPSec-VPN terminal (IP address or host name), IP address of opposite terminal of IPSec (host name) and password, etc., and this stage is to complete all parameter configurations of SA in the first stage.

Configure the second stage of IKE. SA parameters in the second stage are defined by a transformation set; therefore, the configuration of IKE in the second stage should define the transformation set firstly and complete the selection of encryption algorithm, data verification algorithm, etc. At the same time, specify the operating mode of IPSec (transport mode or tunnel mode) and the survival time of data transmission and complete the parameter configuration of SA in the second stage.

Define interested data streams. Use ACL to define the data streams with different characteristics, and we have implemented different security strategies.

Create an encrypted map. Create a named encrypted map, match the data streams to be encrypted, specify IP address of the opposite equipment (host name), and designate the transformation sets to be used in the encrypted map.

Apply the encrypted map to the specified port.

IPSec-VPN running tests

We have operated and configured the simulative network of IPSec security strategy, started to use the capture function of Wareshark data packets on S0/0 link of the connection between IPSec-VPN gateways, and respectively applied the network behavior “ping 10.1.2.1” and “ping 10.1.3.1”, in which the data streams generated by the former belong to the stipulated streams of IPSec-VPN security strategy, so they should be processed by IPSec security strategy, and the processing results are that we only can see the IP addresses of ESP wrapper and IPSec-VPN gateways and other information is encrypted and shielded. However, the data streams generated by the latter are not interested by IPSec-VPN security strategy, so the processing of security strategy is not conducted and we should see the normal information of ICMP data packets and IP address of the original host. The specific results are shown in figure 2. In the teaching process, we can change IPSec security strategy on both sides of VPN system based on this case, use ACL to define various types of data streams, and them apply the corresponding network behavior and generate the corresponding data stream to check different data streams’ different states when passing IPSec-VPN transmission so as to increase the speciality, authenticity and intuitive understandability of the teaching of network engineering.

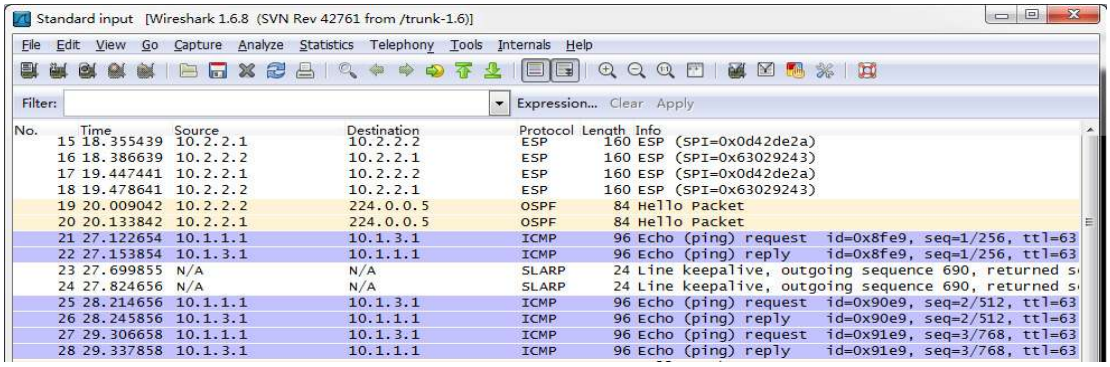

Figure 2 IPSec-VPN data packets

Conclusions

Based on the basic principles of IPSec protocol and VPN technology and combined with the practical needs of network engineering, this paper has put forward the basic framework of IPSec-VPN application case, achieved simulation operation in GNS3 virtual network environment,

tested the transmission characteristics of different types of data streams under IPSec security strategy, and verified the security processing effects of IPSec-VPN on the interested data streams, we let other types of data streams pass through normally. The simulation method and the case can be the reference to the practical teaching of network engineering specialty.

Reference:

[1]Yang Wenwu. VPN Gateway Design and Achievement Based on IPSec[D]，[master's thesis of National University of Defense Technology]，Hunan: National University of Defense Technology, 2008,04

[2]Introduction to GNS3 [EB/OL]. http://www.gns3.net/gns3-introduction/,2012-11-20

[3] The network working group, S.Kent, R.Atkinson.IP Authentication Header[J]. RFC2402, 1998: 144-169.

[4]The network working group, S.Kent,R.Atkinson.IP Encapsulating Security Payload(ESP)[J].RFC2406,1998:34-48.

[5]The network working group, D.Piper. The Internet IP Security Domain of Interpretation for ISAKMP[J].RFC2407,1998:236-264.

[6]The network working group, D.Harkins, D. Carrel.The Internet Key Exchange (IKE).RFC2409, 1998:79-92