Research on meteorological information network security system based on VPN Technology

Chen Jianyun[1]，LiChunyan[1]

[1] Fuzhou Meteorological Bureau， Fuzhou, China

Abstract：In this paper, the concept of VPN and the security technology are studied. In combination with the characteristics of the network, the security technology of the remote access VPN server and the client is discussed, the VPN security system of the meteorological special network is designed, and the VPN network security system of the meteorological network is realized.

1 VPN AND VPN TECHNOLOGY

AVirtual private networks (VPN), a temporary, secure connection through a public network (usually the Internet), are a safe and stable tunnel through a chaotic public network. Generally, VPN is an extension of the intranet, which can help remote users, company branches, business partners and suppliers to establish a credible security connection with the intranet of the company and ensure the safe transmission of data.
Key technology of VPN

1.1. Tunnel technology

Tunnel technology is one of the key technologies of VPN implementation, and it is the technology of another protocol transmission through some protocol, which is realized mainly through the tunnel protocol. It contains three protocols: tunneling, transmission and passenger protocol. Tunneling protocol is mainly responsible for building, dismantling and maintaining the tunnel. The transport protocol mainly transmits the tunnel protocol, while the passenger protocol is the encapsulation of the protocol. Data transferred through tunnels is usually encapsulated and sent to different protocols by means of tunneling protocols. The routing information is provided by the new frame head to ensure that the encapsulated packets are delivered to the destination node through the Internet, and then the original packet is obtained by unsealing.

1.2. User authentication technology

Before the formal connection of the tunnel is ready, user authentication is usually used to confirm the user's identity, so as to realize the user authorization and further resource access control of the system. Generally, the authentication protocol uses a summary technique, which transforms the length of the long message through the HASH function, and maps it to a fixed length summary. However, because the characteristics of HASH function are difficult to grasp, it is more difficult to find the same length digest in different messages.

1.3. encryption technique

In the process of data packet transmission, data hiding is mainly depended on data encryption technology. If the Internet is not safe enough to pass through packets in the process, even if user authentication has passed, VPN is not necessarily secure. In the sending side tunnel, user authentication should first be encrypted and then transmitted. In the receiver tunnel, the authenticated users should decrypt the data packets first and classify the current cryptography according to the difference of the key types, which are divided into two categories: symmetric and asymmetric encryption systems. In practice, usually symmetric encryption is applied to massive data encryption, while public key cryptography is usually adopted for key core data encryption.

Cryptography is usually divided into two categories: symmetric key encryption and asymmetric key encryption.

1.Symmetric encryption technology

Symmetric algorithm, also known as traditional cipher algorithm, means encryption key can be decrypted from secret.The key is calculated, and the reverse is also established. In most symmetric algorithms, encryption decryption key is the same. These calculations.It is also known as the secret key algorithm or the single key algorithm. It requires the sender and receiver to agree on a secure communication.The security of symmetric cryptosystem is mainly determined by two factors: one is that the encryption algorithm must be strong enough.It is not necessary to keep the algorithm secret. It is not feasible to decode messages only according to ciphertext, and the other is the security of keys.The key must ensure that there is enough large key space. Symmetric cryptography

* Corresponding author: e-mail: 385659847@qq.com，515911744@qq.com

requires knowledge based on ciphertext and encryption / decryption algorithm.It is infeasible to decipher the news.

2 Design of VPN security system for Meteorological Network

2.1. The present situation of Fuzhou Meteorological Network

Fuzhou meteorological special network was built in 2000. After nearly twenty years of construction and continuous optimization and expansion, it has begun to take shape.

With the development of the Internet and the popularity of mobile terminals, more and more internal employees have not only been sitting in the office to deal with daily affairs, such as the needs of various types of remote access to meteorological services and applications, such as business staff, family office, and external unit access. At the same time, the occurrence of this network connection also brings new security threats to the information security of meteorological network. In view of the risk of this existence, the weather information network can safely realize the access of remote employees and external units to the meteorological internal network resources through a simple and practical solution, and will not bring new security risks to the meteorological network.

2.2. Safe tunnel treatment

Working principle of SSL safe tunnel. As shown in Figure 1

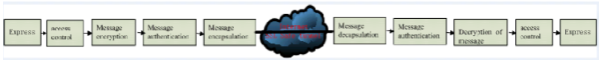

Fig 1. Working principle of SSL safe tunnel.

The transmitter and receiver can be any form of wide area interconnection. SSL VPN device is the main body, mainly building secure tunnel and virtual private network. The client SSL VPN device is its own browser, it is realized by proxy forwarding technology, while the SSL VPN devices on the server side appear in the form of combination of hardware and software, and the hardware platform and VPN processing software are used to implement the function of VPN. When the plaintext of the transmitter enters the SSL VPN device, it is first decided whether to allow it to go out to the public network by access control, and if allowed to go out, it should be determined to be directly out, or should be encrypted and authenticated by the SSL security tunnel to another site of the remote VPN. The message that needs to enter the tunnel is encrypted in accordance with the provisions of the SSL protocol to ensure the confidentiality of the message, and then the message authentication process is carried out by the HMAC algorithm to ensure the integrity of the message and the identiability of the source.

2.3. Establishment of safe tunnel

Before transmitting data on Internet, the Meteorological Bureau staff must coordinate the exchange occurred, such as data encryption algorithm selection and key agreement. A secure tunnel is created by defining the route from source address to destination address from Internet, and using secure communication protocol together.

In the SSL VPN server, after completing the standard TCP handshake and the SSL handshake, there is no connection with the Fuzhou Meteorological Bureau server, and the client initiates a private handshake to determine the Fuzhou Meteorological Bureau server that the client needs to access by handshaking (if the client does not initiate a private handshake, SSL VPN is default. " When the server receives a Web server, the server receives a private handshake request, initiates a request to the college server according to the private handshake protocol; the server receives a response from the server of the Fuzhou Meteorological Bureau or at a time when the private handshake protocol returns a private handshake response. After the private handshake is successful, the server is in the customer's handshake. A safe and reliable tunnel has been built on the server of Fuzhou Meteorological Bureau, and completed the communication of specific application on the tunnel.

The SSL VPN communication handshake process, as shown in Figure 2, is shown in Figure 2. The application first deals with the TCP handshake with the SSL VPN server and establishes a TCP connection; then the SSL handshake is carried out, and the private handshake is used to connect the SSLVPN server to the remote server and to carry out the data transmission; finally, the SSL connection and TCP connection are closed.

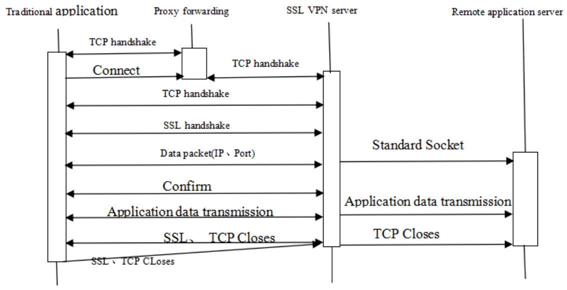

Fig2.SSL VPN handshake communication process

The private handshake process, as the engine of the client application, provides the necessary information for the server, including the servers that the weather bureau wants to visit and the service needs of the employees, and so on.

2.4. Solution description

Meteorological network through the Internet data transmission platform, the implementation of encrypted VPN access to secure access are mainly two: one is IPsec VPN, the other is SSL VPN. The two technologies have their own advantages in different fields. IPsec technology is generally adopted when the fixed site to the site VPN is implemented; SSL technology is usually used when the mobile users who implement the common application are connected to the VPN.

SSL secure access (called SSL VPN) fundamentally solves the problem of remote access to meteorology, and provides secure remote access to internal network resources for remote employees and external units of the weather. At the same time, SSL VPN eliminates the inconvenience caused by remote user's maintenance. At the same time, SSL VPN has the following characteristics.

1.Accessibility

Without changing the existing network architecture, we only use the security function of standard WEB browser to achieve secure remote access. Like other VPN devices in the network layer, the SSL platform is compatible with existing network servers and network resources, without the need for a separate custom development and software integration. The SSL platform greatly reduces the cost of the system deployment. Because the installation of the client software does not exist, it also reduces the cost of the maintenance and management of the business.

2.Safety

The SSL platform provides the overall network security design, completes the transformation of external application requests through a solid system， then fine-grained access control for various connections, and then this security guarantee is not based on the sacrifice of investment, complexity and stability.

3.Extensibility

The SSL platform provides standard application extension interfaces through these standard interfaces to complete seamless integration with third party trusted management systems or single sign on systems and application portal systems. SSL platform makes full use of the existing IT resources of the user.

3 Implementation of VPN security system in Meteorological Network

The network firewall of the weather network deploys the network firewall, and the network in the bureau is logically isolated. The remote users' access to the internal network of the bureau is mainly for the access of some application services. The SSLVPN remote security access system is installed in the DMZ area of the network. On the export firewall, a legitimate routing IP address is mapped for SSL devices so that users of the Internet can be connected to the SSL device normally, and the corresponding security policies are added to the firewall. Remote users can only access the 443 port of SSL device (HTTPS connection), and protect SSL devices and internal servers.

For future network, if we deploy PKI system, we can use X.509 format certificate authentication to achieve remote user access. Remote users first login to SSL devices through WEB browsers, submit corresponding certificates to SSL, and after SSL verifies client certificates, they can query the corresponding LDAP server, get related attributes of the certificate, and make access authorization. In this way, users can access the internal related server resources. The communication between the client's client and the SSL device, using the means of SSL encryption, ensures the secure transmission of these sensitive data on the untrustworthy Internet. The following diagram is a topology map of a SSL device deployed.

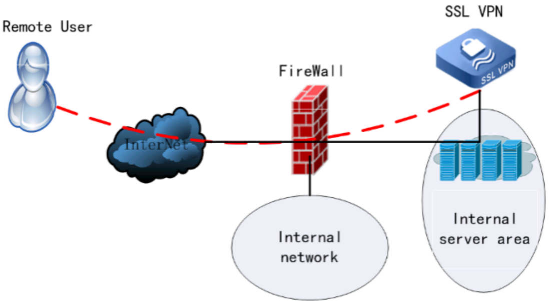

Fig 3. SSL VPN deployment.

3.1. Remote secure access to zero client

SSL remote security access system using the standard WEB browser of the system and the SSL security protocol without the need to install the client.It supported by the browser to achieve secure access to the application server of the enterprise intranet. During the access process, important data is transmitted on the Internet in the form of SSL encryption. SSL system helps remote clients to access internal application servers in three ways.

1.Deep transparent mode.

The access of the deep transparent mode uses the standard WEB mode. The remote user first landed in the SSL system to carry out the related security mechanism inspection and identity authentication. After authentication and authorization, it directly clicked on the related predefined network tags on the SSL application portal's home page to see the access to the internal server.

Access to the core approach supports the following applications:

- Secure web application access: support for content and application based on Web, including HTML, Javascript, DHTML, VBScript, Java applets, etc.
- Secure file sharing access: dynamic Windows and web of Unix file (CIFS/NFS).
- Standard E-mail client access (Outlook Web access).
- Secure terminal access: for Telnet/SSH hosts (VT100, VT320...)

3.2. Client plug-in mode.

In the client plug-in mode, the remote user first landed in the SSL system to check and authenticated the security mechanism. After authentication and authorization, the remote system automatically loaded a small plug-in based on the authority and the access content. This plug-in can redirect the specified network access and SSL the SSL system, and send the request to the SSL system. The request is parsed and the access request is applied to the application server inside the enterprise. This mode can ensure that the existing client applications are unchanged.

Using client plug-in mode can support the following applications.

- Access client / server applications, including native mesSSLing clients (Microsoft Outlook and IBM/Lotus Notes).
- The other is based on fixed service ports, which is a relatively simple application.

3.3. Network layer connection mode

In the network layer connection mode, the remote user first landed in the SSL system to carry out the related security mechanism inspection and identity authentication. After authentication and authorization, the remote system will automatically load a small plug-in. This plug-in can automatically obtain an IP address of the internal network from the SSL system, thus realizing access to the internal network resources. This kind of access and IPSec.

NC can support almost all network applications, including relatively complex video conferencing, IP phone and so on.

4 COMPREHENSIVE REMOTE ACCESS SECURITY PROTECTION

The SSL remote access solution provides a full range of security protection, from the client access, to the data transmission on the Internet, to the SSL access platform, and it is to the resources protection control of the backstage server and other aspects, which provide the corresponding security mechanism.

4.1. Security of access nodes

With the access of remote users, for network administrators, it is equivalent to extending the office network in the Bureau, and how the existing security and security policies of the enterprise are equally effective for the newly connected hosts. SSL can provide a comprehensive solution to check the security policies of the access nodes and implement the corresponding access according to the results of the inspection. Control. And allow administrators to customize the following options

- Open / permissible ports check
- Permissible / unallowed process check
- Hardware features (such as MAC, CPU ID, etc.) check

4.2. Access cache scavenging agent

If remote users are using an untrustworthy remote host and access to the internal network in the Bureau, the browser's cache will retain a part of the access data, which can easily cause accidental leakage of sensitive information. The SSL system provides the function of caching clearance for this purpose. When users login to the internal network, the user can automatically load a caching clearance agent locally, in the user. In the case of normal cancellation or abnormal exit, the session data and temporary files left by the access of the system are cleared. It ensures that sensitive information will not remain on the client host.

4.3. Authentication for landfall users

The SSL system supports the use of digital certificates, which can be used individually to verify the user's identity by the client's digital certificate, thus avoiding the inconvenience of entering the username / password. At the same time, the SSL system also supports a variety of authentication servers (including RADIUS, LDAP, Windows NT Domain, Active Directory, etc., including ActivCard ActivPack), RSA SecurID, and client digital certificates.

For the network in the Bureau, if the PKI system is established in the future, we can authenticate the client by means of the certificate so that we need to apply for a digital certificate for the SSL system (and the root CA certificate into the SSL system). In this way, only the user who passes the correct digital certificate can only pass the authentication of the SSL system and have the backstage server. Access rights. At the same time, the SSL system also supports the query of the status of the certificate by CRL downloading or OCSP protocol. In this way, the invalid certificate cannot be authenticated by the SSL.

At the same time, we can also use the way of user name, password and digital certificate sorting. After a failed authentication, we can log in through the second authentication. The SSL platform also provides protection against user side password cracking, in order to prevent dictionary detection attacks. The system has limited the frequency of multiple landing requests. And the detection of the security of the first set passwords..

REFERENCES

1. cuikai. SSL&TLS Dosingning and BuildingSecure System[M].China Electric Power Society. 2002.44~73
2. Jia HuiNa,Qiu ZhengDing.Advantages and prospects of SSL VPN Technology[J].Computer security.2005,8:34~35.
3. Bao LiHong, LiLiYa.Technology research based on SSL VPN[J].Jiangnan Computer Institute.2004,5:3~40.
4. Zhang Mei.Key technology research and system design of SSL VPN.2012(02):78-79.
5. Rongfang yang. Application of Internet of things in meteorological disaster prevention and mitigation. Atmospheric composition and climate change.2012(S16).