A Three-Step Strategy for Recommendation in Mobile Police Video Secure Access

Xinming Yin\textsuperscript{1,2}, Yi Guo\textsuperscript{1*}, Zhiwei Cao\textsuperscript{2} and Min Xiong\textsuperscript{2}

\textsuperscript{1}School of Computer Science and Engineering, East China University of Science and Technology, Shanghai 200237, China
\textsuperscript{2}The Third Research Institute of Ministry of Public Security, Shanghai 200031, China
Email: guoyi@ecust.edu.cn

Abstract. Mobile police video security access link is an important boundary channel to ensure the secure and trusted access of mobile video in the private video network. Therefore, this paper proposes a three-step strategy for access control, encrypted transmission, and wireless video security inspection. While carrying the ability to carry higher video streams, it is both safe and reliable, and has strong scalability in performance. This paper analyzes the access mechanism of SSL VPN in encryption, identity authentication and resource access control. Proposes a mobile police video security access link solution based on SSL VPN for network clients. Respectively presents a secure access solution for wired video and wireless video. And a load balancing access scheme based on NAT address translation is designed. Finally, a test scenario for the maximum number of concurrent users and server bandwidth performance is designed, implemented and analyzed. In actual application, the trial projects have been highly recognized by public security customers.

Keywords. Three-step strategy; open secure sockets layer; mobile police video link; load balancing.

1. Introduction

With the development of internet economy, enterprise customers are more and more widely distributed, the number of cross-border customers is also growing, the traditional end-to-end access method based on fixed location can no longer meet the application demands of users. Under such a circumstance, the virtual private network (VPN) has won the favor of more and more enterprises for its advantages in economy, security and scalability in the network. Similarly, for the characteristics of mobile video applications, VPN technology should play a bigger role in the access of video resources between different network domains.

2. Security Mechanism and Implementation Mode

SSL VPN technology is based on the SSH protocol. It mainly guarantees users secure and efficient access to data information in different domains through mechanisms such as digital certificate authentication, data security encryption and message integrity verification.

2.1. SSL VPN Security Mechanism

In the process of accessing mobile police wireless video, in order to ensure that public security intranet users can securely and quickly access the video resources of mobile police terminals, and to effectively
and reasonably control the access rights of public security network users, the SSL VPN technology mainly uses the following security strategy.

1) SSL encryption. The proposed SSL VPN system is an improvement based on the OpenSSL software package. OpenSSL’s cryptographic algorithm library contains complete OpenSSL certificate management, key management, and the standards implementation related to cryptographic algorithms. Among them, SSLeay is the core of the OpenSSL, and basically the standard algorithms have been included, such as symmetric encryption algorithm, hash algorithm, and asymmetric encryption algorithm [1, 2].

2) SSL authentication. To guarantee mobile police terminal security access, mobile police terminal to be accessed will be authenticated first, FAD authentication mode is implemented in SSL VPN, bidirectional authentication mode is designed between mobile police terminal client and background service.

And SSL certificate includes information of login user and police terminal, such as an encrypted digital certificate and a public key. The public key can decrypt the information in the digital signature and verify the integrity of the certificate through the decrypted value. The SSL certificate in this article is mainly generated by CA, including root certificate, site certificate and client certificate. The site certificate is set on the server and the client certificate is set on the mobile police terminal. Both certificates are generated through the root certificate that is also in charge of two-way authentication.

3) SSL access resource control. The characteristics of SSL VPN with wider granularity selection are fully considered, access to the file directory, URL, and IP address and port number can be controlled.

2.2. SSL VPN Implementation Type

There are three common customer implementation types for SSL VPN:

1) Clientless mode, which is mainly accessed by a web browser and only protects web traffic.

2) In THIN client mode, the client usually downloads the ActiveX software to the client. This mode allows a small subset of non-Web applications to be securely transmitted through VPN encrypted channels, such as SMTP and SSH.

3) In the network client mode, the client needs to download an IP client, which is responsible for establishing SSL communication connection with the SSL gateway. SSL VPN based on this model can protect traffic in network layers [3-5].

In response to the needs of police mobile terminal wireless video applications and the high security requirements of the public security intranet, this article uses the SSL VPN implementation mode based on network customers. At the same time, according to the relevant standards of the Science and Technology Information Bureau of the Ministry of Public Security china, the current wired video security access solution uses a 2+1 working mode, including a video front-end machine, a video gatekeeper, and a video back-end machine [8, 9].

3. Research on Video Access Proposal

To guarantee video data secure transmission between different domains, wired and wireless video security access is proposed respectively on the basis of the actual application of mobile police terminal.

3.1. Wired Video Security Access Proposal

As a branch of public security border access, the wired video security access solution is a powerful guarantee to ensure the safe and efficient connection of video services between different network domains of public security. At the same time, according to the relevant standards of the Science and Technology Information Bureau of the Ministry of Public Security china, the current wired video security access solution uses a 2+1 working mode, including a video front-end machine, a video gatekeeper, and a video back-end machine [8, 9].
3.2. Wireless Video Security Access Solution
The wireless video security access is a video security access method proposed for mobile police video applications. It is mainly responsible for connecting mobile video resources to the trust network through wireless access. The wireless video access method adds the SSL VPN function on the basis of the wired video security access method. The mobile video data is transmitted to the public security intranet securely and efficiently through WiFi or 4G network [10, 11].

4. Mobile Police Video Link Integration
Mobile police video application is an important support in the development of public security informatization, and it is also a widely used business in the public security industry. At the same time, mobile police video applications have relatively high requirements for security and link bearing performance. Based on the above requirements, this article proposes a complete set of integrated solutions for mobile police video links based on SSL VPN, and designs a load-balanced access proposal based on NAT address translation. Finally, this paper conducts experimental design and performance analysis of the entire set of access proposals.

4.1. Integrated Solution of Mobile Police Video Link
For the security and efficiency requirements of mobile police video applications, a complete set of mobile police video link access solution is proposed for mobile police video applications, which are mainly composed of a video security access system, a security VPN access gateway, and a video streaming media platform.

The VPN gateway is the core of the entire set of links. It is responsible for SSL identity authentication and access control of the mobile police equipment of the video private network, and at the same time securely encrypts the video stream transmitted by the mobile police equipment to ensure the security of the private network video resources. Efficient transmission. The video security access system is the boundary access part of the entire link. It is responsible for the identity authentication of users accessing video resources in the public security intranet, as well as the protocol and format check of the transmitted video stream, and at the same time guarantees the two-way transmission of video signaling and one-way transmission of video streams [12, 13].

4.2. Application of Load Balancing in Integrated Solutions
Due to the relatively large demand for video applications for mobile police terminals, basically always a large number of public security intranet users request services to access remote video. It is difficult for a single SSL VPN server to withstand such a large load, resulting in many users’ requests not being able to respond in real-time. In order to improve the quality of service, a load balancing proposal is proposed, deploying multiple SSL VPN servers to the mobile police video link, so that a large number of video retrieval requests are directed to different SSL VPN servers, as a result each server can carry approximately the same video application request.

In view of the characteristics of mobile police terminal video application, it is adopted that the load balancing proposal of NAT address translation for SSL VPN service system.

For the video access signaling sent from the public security intranet, it first enters the video private network area through the video security access system, and then sends it to the load balancing server through the border switch for the second exchange. The load balancer observes the source IP of the packet and looks up the session list. If there is no session, load balancing is performed, and the optimal gateway is allocated for processing according to the load balancing algorithm, and the source IP and gateway IP are recorded in the session list; if there is already a session, the session is maintained and the gateway IP of the corresponding session is found. And it is handled by the gateway IP. During the forwarding process, only the destination NAT is done, and the load balancer IP is mapped to the real gateway IP.

The packet forwarded by the load balancing server passes through the switch and reaches the real SSL VPN server. After the SSL VPN server receives the forwarding packet, it still thinks that the request
signaling packet for viewing the video is directly sent from the border access network (video security access system), and the corresponding encryption and identity are carried out in the same way as without load balancing. Authentication, inspection, etc., followed by video request signaling through the virtual channel opened by the SSL VPN service, and then through L2tp access routing, GGSN, etc. to reach the destination address, request private network video resources.

The mobile police video terminal receives the video access signaling and responds to the media data stream or video signaling. The SSL VPN client of the mobile police video terminal performs SSL encryption, SSL authentication, and SSL resource access control on these video resources and video response signaling. Then the encrypted data enters the SSL VPN server distributed by the load-balancing server through the Internet. The SSL VPN server performs identity authentication and decryption on these data packets. The restored video stream and response signaling arrive at the border switch and enter the border access area. (Video security access system), and finally reach the public security intranet.

In summary, in the load-balancing access proposal of the mobile police video link, the request signaling sent by the client of the public security intranet must allocate the optimal SSL VPN gateway through the load-balancing algorithm of the load balancer. Then, the media server does not need to go through the load balancer when forwarding the video stream, and directly enters the border access area through the SSL VPN gateway, thereby strengthening all links of the entire mobile police video access link, and ensuring the safe and efficient transmission of the data stream.

4.3. Performance Analysis of Mobile Police Video Access Link
The carrying performance of the mobile police video access link is a technical indicator closely related to the public security intranet users, and also an important criterion for evaluating the overall effect of the access proposal. In the access proposal designed in this paper, in order to ensure the function of secure encryption of video data, the secure VPN access gateway will inevitably lead to the impact on the performance of the entire mobile police video access link, so it is also a key element affecting the entire secure access link. In view of this, this article aims at the uniqueness of video data, try to use BF, CBC and other symmetric encryption algorithms in the process of data encryption, because the encryption speed and encryption efficiency of this type of algorithm are relatively high, and the amount of calculation is small, which is more suitable for processing Businesses with large amounts of data [14, 15].

In summary, in the case of ensuring the smoothness of WiFi or 4G network, this paper designs a test plan for the maximum number of concurrent users and server bandwidth performance, and analyzes the test results.

4.3.1. Max Number of Concurrent Users. The maximum number of concurrent users is a key indicator to measure the performance of the mobile police border access link, and determines how many intranet users can access the video resources of the private video network at the same time. In view of this, this paper has designed the following test plan for the maximum number of concurrent users.

(1) At first, run a simulated client test program, which is mainly used to simulate the process of logging in to the VPN server for public security network users. Ensure that the simulated client and the SSL VPN server complete the password authentication first, and then use the CA certificate for two-way ID authentication, and finally ensure process communication between the client and the background service.

(2) Create 500 simulated public security network users in the SSL VPN server background database, and randomly put 50 users into a group.

(3) Build a virtual machine for testing to ensure when the test script is run, a group of users, that is, 50 users log in concurrently

(4) After each user logs in, simulate playing a 2 Mbps SD (standard definition) video on demand, and observe the video stream if smoothly.

(5) Continue the above steps until the video stream is noticeably stuck.
The SSL VPN server for the mobile police video access link can hold up to 350 simultaneous users who log in at the same time, and can ensure that these users will not be significantly stuck when accessing the 2 Mbps standard-definition video of the private video network.

4.3.2. SSL VPN Server Bandwidth Performance. The bandwidth performance of the mobile police video access link is the basic condition for ensuring the normal operation of the wireless video access service. On the one hand, it can ensure that the users of the public security intranet can safely and quickly access the video private network resources; on the other hand, it can ensure that users of the public security intranet easily and quickly access other corresponding functions of the mobile police terminal.

The specific test steps are similar to the test procedure for the maximum number of concurrent users. In the bandwidth test, taking a normal video play smoothly for example, and then uses a third-party software Iperf to simulate a stress test for video data, when the bandwidth reaching the limit, check the packet loss rate of the corresponding SSL VPN server and the smoothness of the video stream observed.

The maximum bandwidth that the SSL VPN server for the mobile police video access link be able to carry is about 700 Mbps. If you continue to add video stream data, the packet loss rate will increase and the video stream will be severely stuck.

5. Conclusion
Mobile police video security access link is a very important business in the development of public security informatization, and it is also a key technology related to whether the private network wireless video stream can be safely and efficiently transmitted to the public security intranet. In view of this, this paper first studies the security mechanism of SSLVPN, and at the same time aims at the application characteristics of wireless video, and proposes an SSL VPN implementation model based on network clients. Followed by SSL VPN’s unique OpenVPN secure encrypted tunnel technology and wireless video security access solution.

This article designs a complete mobile police video security access link. In view of the characteristics of mobile police terminal video application requirements, this paper proposes a load balancing technology based on NAT address translation, which expands the performance indicators of the entire access scheme.

This paper also conducts simulation experiments and performance analysis on the entire set of access schemes. It is verified that the access schemes proposed in this article can well meet the safe and efficient access of a large number of video resources between different network domains, reflecting the high performance of Good encryption function.

The program has been piloted in a public security department of a certain place, and the effect is good. There are still some deficiencies in this article, mainly reflected in the versatility of SSL VPN encryption strategy to be improved, which needs to be considered in the subsequent research.

Acknowledgments
The projects funded by this paper are: National Key Research and Development Program (2018YFC0807105, 2018YFC0807106); Shanghai Science and Technology Talent Program (17XD1420400).

References
[1] Wu Y 2014 Research and Implementation of National Secret SSL Secure Communication Protocol (Xi’an: Xidian University).
[2] Lu H 2017 Symmetric searchable encryption scheme port information network security with hidden search mode Netinfo Security (1) 38-42.
[3] Yu D, Shu M and Tan C 2011 Research and implementation of mobile SSL VPN system based on Socks5 proxy Computer Science 38 (1) 119-122.
[4] William S 2010 Cryptography and Network Security Principles and Practices (NJ: Prentice Hall).
[5] Zhu Y and Gui Z 2014 Research and implement of VPN key technology—Based on OpenVPN Computer Security (1) 23-27.

[6] Likhar P, Yadav R S and Rao M 2011 Securing IEEE802.11g WLAN using OpenVpn and its impact analysis International Journal of Network Security & Its Applications 3 (6) 97-113.

[7] Fu X, Lu Y and Shao Z 2016 Research on information security simulation experiment platform technology of public security video surveillance system Netinfo Security (9) 56-59.

[8] Huang K, Chen X, Kang Y, et al. 2015 Overview of intelligent video surveillance technology Chinese Journal of Computers (6) 1093-1118.

[9] Chen X, Jin Y and Yang T 2015 Research on mobile video data evaluation model in 3G network Computer Science 42 (9) 86-93.

[10] Wang Q 2014 Design and Implementation of the Border Access Platform of the Public Security Information Communication Network (Xiamen: Xiamen University).

[11] Baranyi S 2014 The development of the national police, public security and the rule of law in Haiti Powder Technology 256 (2) 361-366.

[12] Fan F and Yang G 2015 Optimized coverage algorithm for wireless video sensor networks based on quantum genetic algorithm Journal of Communications 36 (6) 98-108.

[13] Niu L 2016 Research on expressway wireless mobile video surveillance system based on 3G network Highway Transportation Science and Technology (4) 277-279.

[14] Li Z, Liu D, Huang X, et al. 2016 Design and implementation of secure access equipment based on national secret algorithm Netinfo Security (11) 19-27.

[15] Usui T, Kitatsuji Y and Yokota H 2013 a study on traffic management cooperating with IMS in MPLS networks Telecommunication Systems 52 (2) 671-680.