Design of SSL VPN system based on RBAC access

FAN Ya-qin [1,a], ZHANG Ge [1,b] LI Fei-fei [2,c,] , ZHANG Xin[1,d]

[1.]College of Communication Engineering,Jilin University Changchun 130012 china

[2.] Jinzhou Branch Company of China United Network Communications Co., Ltd.121010 china

[a.]fanyaqin_joy@163.com，[b].404360310 @qq.com，

[c].fei19850131@163.com,[d].940614745@qq.com

Keywords: SSL VPN access control technology control model

Abstract. Abstract: in order to solve the access control system loopholes, can appear the problem of chaotic management, security failure and conflict of competence, this paper studies the access control model, on the basis of the design of a SSL VPN oriented access control system, the authentication module, access control module, role access module and security detection module design. The realization technology of system user identity. This has practical reference significance to the personnel security technology research network.

Overview

SSL VPN is an application layer based on VPN technology, has now become the preferred security platform of remote access. Access control has become an important means of security to prevent illegal access, RBAC access control model is now the mainstream access control model based on one. Access using the RBAC design of the principle of SSL VPN control module. The following will visit on two aspects of the overall design and related technology of its realization from SSL in VPN system.

The overall design of the SSL VPN system based on RBAC access

Accessed using the principle of RBAC model to design the SSL control of VPN system model. Need to design content mainly has: distribution between roles and permissions, permission assignment relations role and access resour[1].

The RBAC module SSL VPN system.

In the SSL VPN server function module, system management, user login, security check, RBAC and forwarding resource. As shown in figure 1. System management module for the role of user distribution, to obtain the proper permissions through roles, and the control request of cyber source and service users. Role of control is based on the user identity authentication. The login module main function is to identify and verify the identity of the user request through the user login. Safety detection module is used for security detection and assessment of client state. The main role of resource forwarding module is to process the network data transmission[2-3]. Identity authentication module first in a direct way by username / password for identity authentication of the user, and then the identity authentication in an indirect way through the digital certificate used for users of the SSL VPN server.

RBAC module is the core module of SSL VPN system, it must interact with other modules in the system, extracting the necessary information for dynamic authorization of users from these modules. The login module needs to provide the user login information, system management module need to provide user roles configuration information. Authorized to determine the allocation of resources, so the RBAC module is the key to achieve fine-grained access[4]

Published by Atlantis Press, Paris, France.

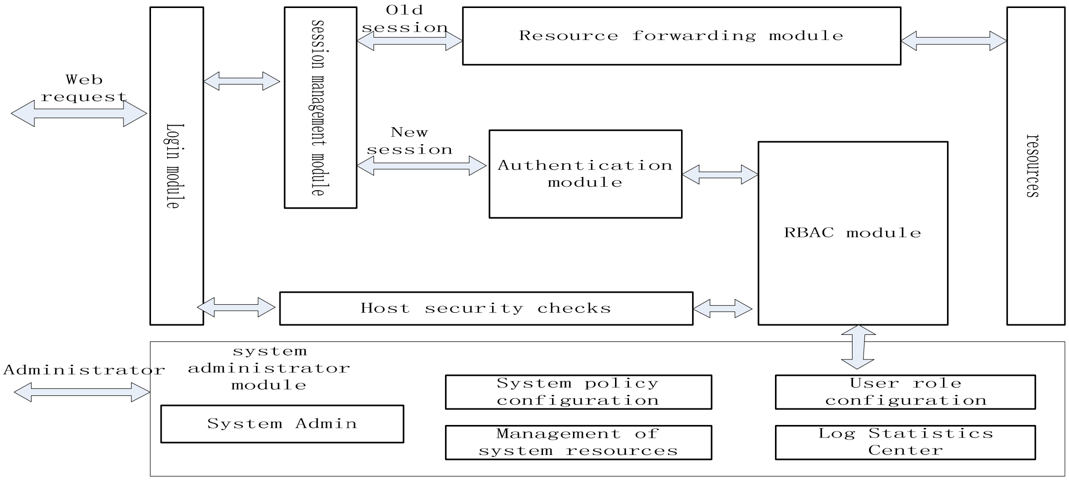
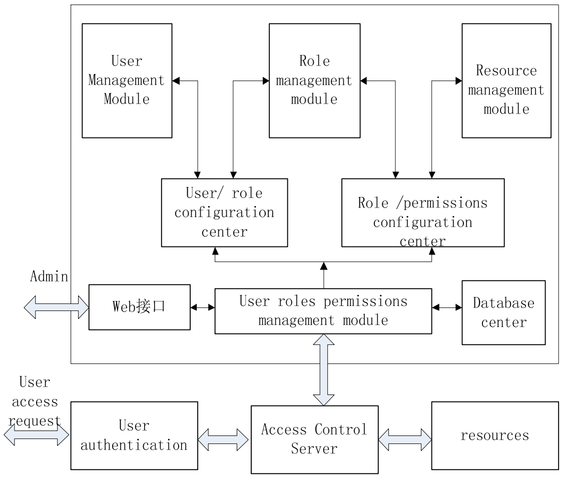


Figure 1 SSL VPN overall function structure chart

Structure design of RBAC module

RBAC can be divided into four modules: the user authentication module design, access control server module, user authority management module and host security check module. Figure 2 describes the main module structure diagram of RBAC module.



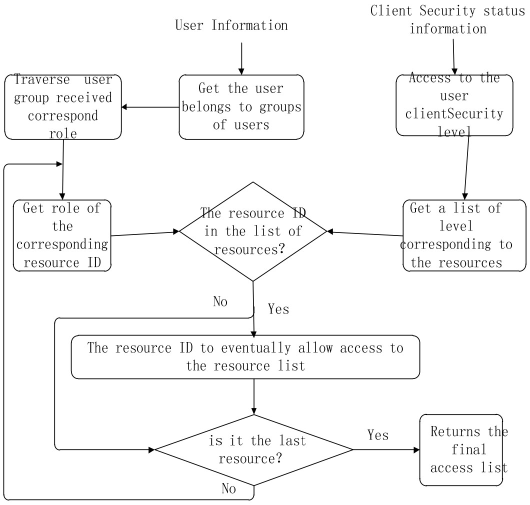

User Information
Client Security status information
Traverse user group received correspond role
Get the user belongs to groups of users
Access to the user clientSecurity level
Get role of the corresponding resource ID
The resource ID in the list of resources?
Get a list of level corresponding to the resources
No
Yes
The resource ID to eventually allow access to the resource list
is it the last resource?
Yes
Returns the final access list
No

Figure. 2 RBAC diagram of the internal structure of module

Figure 3 Access Control Process

Design module of user identity authentication

We can through the digital certificate in PKI mechanism to the two sides with the SSL protocol communication authentication, SSL VPN system is designed in this paper is to use this way to authenticate the client and the server, and then loaded on socket communication SSL protocol, the communication data encryption, to prevent data from being illegally eavesdrop or tamper with.

PKI (Public Key Infrastructure, public key infrastructure) is a key management platform, it follows the established standards, provides cryptographic services including encryption, digital signature, certificate and key management, a complete set of services for all web applications. Simply put, the PKI is relying on security service platform to build public key theory and technology[5-6]. This module, this paper to complete the function of identity authentication communication SSL VPN system on both sides of the design of a simple PKI system. In the PKI system planning, architecture needs to consider the key CA. CA as the certificate issuing authority, which is responsible for issuing the certificate, certification, management has issued a certificate, can be said to be the core of PKI. CA to develop strategies and specific steps to find, identify the identity of the user, but also to sign the user certificate, in order to ensure that the right holder's identity and public key.

Access control server design

Access control decision is mainly rely on the server to implement access control. As the core part of SSL VPN system on the intranet resources access control, its main role is to respond to the legitimate user access to a resource request, will be a list of resources generated to the user. In the specific implementation, access to SSL VPN system control process can be divided into the following steps:

(1) according to the security level of safety inspection by the client SL VPN server.

(2) according to the landing system obtains the user ID, get SSL VPN user or the user group corresponding roles, roles found corresponding resources, generate resource ID, generate the list of resources.

(3) the security level user security level of client and have access to resources, if greater than or equal to the resource into resource list, if less than it would not join the list of resources.

(4) after the above steps, can generate the resources that a user can access list [7].

Access logic diagram detailed as shown in figure 3.

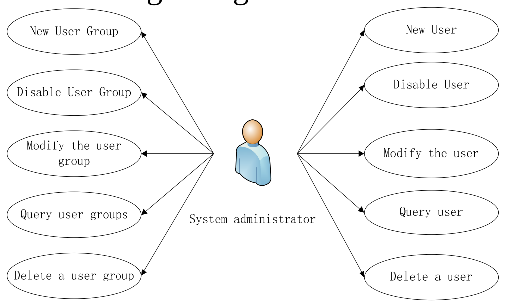


Figure 4 for the user and user group management

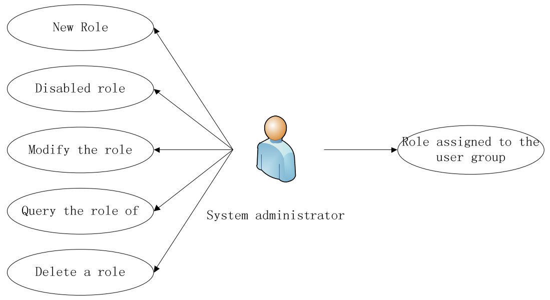


Figure. 5 of role management

In the RBAC system, the conversation is key, because the whole process user access to network resources is accomplished through the session [21], access control server forward the user access request will set up an ID and a unique session, the session will not only access control decision mechanism and system resources together, also record include the user identity information, access to information resources information session.

Design of user authority management module

The RBAC system is composed of management module to implement, management module needs to realize user \ \ user group management, role management, rights management, resource management.User authority management module can be divided into user management module, the role management module:The user \ / user group management module: user authentication mechanism used to store user identity information, so the establishment of user identification module is very important, after all, the system is the user end user. System to the user and user group management Abstract as shown in figure 4.Role management module: the main function of the role to create, edit and delete operations, and establish and maintain a role hierarchy relationship. The system administrator of role management Abstract as shown in Figure 5.Resource management module : the need to set up system resources, in the establishment of resource permissions. Based on the above analysis module, management of user authority management module of the whole system by user and user group a many-to-many relationship, the user group and the role of a many-to-many relationship, role and resource many-to-many relationship to complete. Their relationship can be abstracted as shown in figure 6.

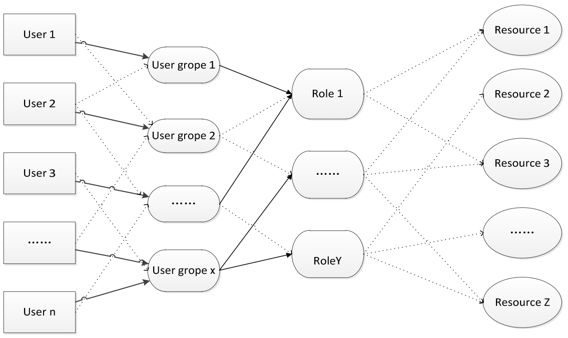


Fig. 6 users, groups of users, roles, resources of organizations

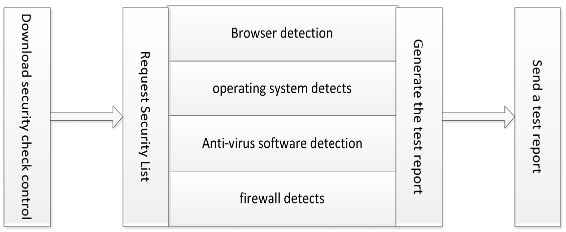


Figure7 the host security check

Design of host security check module

SSL VPN system uses a tunnel encryption technology, firewall and antivirus software can not detect the tunnel encrypted data, coupled with the access mode of SSL VPN support Web, port forwarding agent and virtual NIC technology, which further increases the safety risk. Some of these features may catch malicious attack SSL VPN server to bypass the firewall. In addition, SSL VPN supports the user in the browser access to different terminals, if a user host malware, hidden virus may infect to the internal network. So, the client host security check SSL VPN system is very important. In the access control decision mechanism, security to security check module design requires user permissions and terminal equipment. As shown in Figure 7 the design host security check module.

Analysis of SSL VPN server receives a safety monitoring report, according to the security level previously set safety assessment mechanism for the allocation of the host. The whole system and access to resources is decided by the security level user role and host.

Summary

In this paper, the analysis and the design and implementation of a VPN system based on SSL RBAC access, introduces the design idea and design scheme, focusing on the module of user identity authentication system based on user authentication, CA authentication and implementation plan, ensure the reliable communication of SSL.

Reference

[1] Ouyang Kai. Access control model for VPN and related technology research [D]. Wuhan Huazhong University of Science and Technology 2006.

[2] Duan Zhuoran. Design of SSL VPN system user authority management module and the realization [D]. Beijing : Beijing University of Posts and Telecommunications, 2008; 41 – 45

[3] Bian Changxi. Design of Web information security channel SSL protocol and Implementation Based on [D]. Ji'nan: Shandong University, 2008

[4] Wang Qian, Zhou Jian. VPN tunnel technology and implementation of SSL based on [J]. network security, 2007.8:23-25.

[5] Xu Bo . Research on the SSL VPN access control model. [D] Zhejiang University of Technology, 2009

[6] SHOE[EB\/OL].http:\/\/www.cs.umd.edu\/projects\/plus\/SHOE, 2006-12-8.

King [10] applet .RBAC technology in the management system of the research and application of [D]. Wuhan: Wuhan University of Technology, 2008

[7] Xu Bo . Research on the SSL VPN access control model. [D] Zhejiang University of Technology, 2009