The Network Security Regime for the Hybrid Connection of Healthcare Entities

IP Chon Hou, PUN Sio Hang, VAI Mang I, MAK Peng Un
Department of Electrical and Computer Engineering
University of Macau
Macau, SAR, China

Abstract — **The rapid development of the blooming city requires to expand the government healthcare services for the public because of increasing inhabitants. Additional temporary government healthcare service is set up within a university having an operating hospital in order to solve the urgent requests of the mass amount of the inhabitant. This has resulting resources (medical equipment and IT services) sharing by these healthcare entities but independent operations should be maintained. In order to keep the privacy and security of the digital data and patient data, this paper proposes a method of creating a new subnet as common network area for sharing the resources; while maintaining their independencies at the same time. We have added the network security appliances (firewalls) connecting to the healthcare entities. Through the features of network address translation (NAT), network policy and access control list, this common subnet with hybrid connection (university hospital network and the government hospital network) can accessed by these entities via the specified IP addresses. As a result, the existing IP addresses for each healthcare entity network can be retained, and providing the secured method to grant the access right to the common area to share the digitalized medical resources. In order to protect the security of the cooperated hospital's internal networks, unauthorized traffic into and out of the subnet is blocked or restricted by firewalls as per policies configured.**

Keywords- Healthcare Information Systems, Hospital Network, Security, NAT, Network Policy

I. INTRODUCTION

The rapid development of the city and the expansion of the inhabitants increase the pressure of providing more healthcare services. For a long vision, the government has planned to build a new hospital to fulfill the requirements of the healthcare services for the public. However, a hospital cannot be established in short time. In order to satisfy the near-term demand, a temporary governmental healthcare service is setup within a university hospital because the existing resources of the university hospital can cover the urgent public medical service demands.

This cooperation, nevertheless, is a mutual beneficial proposal especially for the welfare of the general publics. However, these hybrid hospital services create technological challenges to the daily operation of both entities. The university hospital belongs to a privately own comprehensive university; while the governmental medical service is designed for general public. Among the challenges, the network security of the connection between the entities is one of the main impacts for the operating of the hospitals. Moreover the online services of hospital systems such as Health Information System (HIS), Laboratory Information System (LIS), Picture Archiving and Communications System (PACS), and the privacy of the patient data should be secured during the cooperation between the hospitals [1]. The government hospital will use the medical equipment of the university hospital for the public healthcare service, so that the government hospital should access and update the inspection reports generated by the university hospital. For this purpose, a new subnet is created for sharing the inspection reports between the healthcare entities. The aim of this paper includes the design and implementation of the network connection with the following features:

- the availability and security between the hospital networks;
- Non-interruption of the existing hospital system operations.

II. NETWORK INFRASTRUCTURE

A. Existing Network Infrastructure Background

The existing network infrastructure for the university hospital is a 3-tier network design: core network, distribution network, and access layer. The current university hospital network adopts virtual LAN (VLAN) technology [2] for separating the subnets for different hospital administrative offices, clinic departments and laboratories. The access switches in different levels of floors are connected to the distribution switches; while, the distribution switches in the dedicated levels of floors are connected to the core network switches with redundancy. The users can access to the university hospital network and the server farm of the core network by connecting the workstations (clients) to the end-points of the access switches. The entire network infrastructure of the hospital is designed as the private Class A network, which has the high capacity and can have flexibility for the future expansion.

B. Target Network System Integration

For the cooperation of the hospitals, which have their own running network infrastructures, we desire to minimize the risk to disturb or interrupt the running environment. Figure 1 displays the network infrastructure for a subnet accessible from

978-0-7695-4706-0/12 $26.00 © 2012 IEEE
DOI 10.1109/iCBEB.2012.431

two cooperated hospitals. It contains two firewalls and a common area, serving as a private Class B network, for connecting the university hospital and the government hospital. By applying network policy for the connection, the specified workstation clients of the university hospital can grant the access right to the server and the designated network system of the government hospital and vice versa in the common area of the joint common network area.

III. NETWORK CONNECTION DESIGN AND IMPLEMENTATION

For the design and planning for connecting the hospitals, NAT with network policy is adopted since NAT having the following advantages:

- Security - Keeping internal IP addresses hidden discourages direct attacks.
- IP routing solutions - Overlapping IP addresses are not a problem when using NAT.
- Flexibility – Changing the internal IP addressing schemes without affecting the public addresses available externally; for example, for a server accessible to the Internet, maintain a fixed IP address for Internet use, but internally, can change the server address.
- Enhance home network security by limiting the access of external computers into the home IP network space.

A. Target Network Infrastructure Design

The existing network of the university hospital is daily operating, so the feature of NAT for connecting to the government hospital is designed in order to eliminate the collision of the running network environment. Both of the healthcare organizations are connected with network security appliances. For the university hospital side, there are two firewalls connected in redundancy with active-standby configuration. The redundancy configuration can prevent from single point of failure of the network security appliances and thereby increasing the reliability of the data network. The network interfaces are configured for redundancy for fail-over status. The interfaces of the firewalls are then configured with inside and outside network, following with NAT and Access Control List (ACL) [3].

B. University Hospital Network Firewall Implementation

Herewith the selected configuration for the university hospital firewall, please see Table I for the NAT table:

- Configure the fail-over interface IP of the firewall for the redundancy of the firewalls
- Configure the inside network interface IP with standby as Subnet-A-IP-1 for the inside network interface: security-level 100
- Configure the outside network with interface IP of Subnet-B-IP-1 for the outside network interface: security-level 0
- The dynamic NAT is applied for translating the inside network of Subnet-A-IP-2 --- Subnet-A-IP-4 to the outside network Subnet-B-IP-1
- Add the route for connecting to the inside network: 0.0.0.0 / mask: 0.0.0.0 by the core network interface connecting to Subnet-A-IP-1

For the core network of the university hospital, we add the VLAN interface and routing connect to the firewall:

- Create an VLAN interface connecting to the IP address of Subnet-A-IP-1
- Add the routing to the outside network of Subnet-B by Subnet-A-IP-1

C. Government Hospital Network Firewall Implementation

For the government hospital side, the inside network of Subnet-C-IP-2 serves as IP address of the server of the subnet. The outside network of the firewall with the gateway interface assigns with Subnet-B-IP-2. Please see Table II for the NAT table.

- Configure the inside network with interface IP connecting to Subnet-C-IP-1
- Configure the outside network with interface IP connecting to Subnet-B-IP-2
- Static NAT is applied for translating the server located in the inside network of Subnet-C-IP-2 into the “public address” belong to the outside network of Subnet-B-IP2
- Add a route connect to the inside network by: 0.0.0.0 / mask: 0.0.0.0 by the interface connecting to Subnet-C-IP-1

For the core network of the government hospital:

- Create a VLAN with IP address connect to the inside network of Subnet-C-IP-1
- Add a route to the public area network of Subnet-B by Subnet-C-IP-1

For the design of dynamic NAT of the university hospital, the IP addresses of the workstations in the internal network will be translated to one external IP address only. So, the server in the public area of sharing side only receives requests from the university hospital with only one IP address. In this case, only one IP address will make higher security than with IP addresses pool behind the firewalls of the university hospital [4].

D. Policy For The Network Connection Between Hospitals

The access control list (ACL) is applied in order for the workstation clients on the specified VLAN in the university hospital to have access right to the outside network (common access area of the connected network) with the government hospital network. The pseudo configuration of the firewalls of the university hospital will be:

- access-list inside_access_list_in extended permit ip host Subnet-A-IP-2 netmask any

- access-list inside_access_list_in extended permit ip host Subnet-A-IP-3 netmask any
- access-list inside_access_list_in extended permit ip host Subnet-A-IP-4 netmask any
- For the government hospital side, the access control list will only permit the specified IP address of Subnet-B-IP-1 to access the server.

Because of the operating and production of the existing network of the university hospital, it is better for using NAT to translate the existing IP address to access to the common area of subnet connecting to the government hospital. The NAT can retain the existing IP address for the hospitals operation.

Since both entities should have the NAT feature to translate the inside network to outside network of the network equipment, the specified firewalls or the routers with firewall features are recommended for protecting the network attacks as well. As a result, both hospitals can maintain their access control lists (ACL) for permitting the only specified workstation clients or server to grant access to the sharing pool of the subnet.

IV. CONCLUSION

In order to reduce the pressure of explosive demand of increasing healthcare service, the cooperation of the healthcare entities can share the healthcare resources for the government hospital with carefully designed regime. Since most of the healthcare resources are digitalized and connected with the network systems, an additional subnet for sharing the medical resources between the healthcare entities is carefully design and implemented. The advantages of network address translation for the common area of subnet can share the digitalized medical resources; and can be hidden the entities' internal networks.

Considering to minimize the disturbances of the existing operating network and to retain the original IP addresses for the hospitals, the NAT technology is used for translating the existing IP addresses. Hence, the cooperated hospitals can keep their data and patient privacy in their internal networks, and can connect to the specified services for sharing the healthcare resources. For the security reason, the adopted network policies for the specified workstations and PC clients can grant the access rights and permit to connect to the common area of the subnet of the connected network infrastructure. In order to increase the security of the existing running networks, government hospital cannot access the other workstation's IP addresses behind the firewall of the university hospital. If the university hospital hosts attempt to initiate a connection to a mapped address, which is not currently in the translation table, the adaptive security appliance will drops the packet. So far, under the implemented network security regime in an emergency clinic fashion, both healthcare entities can operate smoothly without interruption and network security problem reported for over half a year.

For the future consideration of increasing the workstations or servers with the healthcare organizations, one can simply configure the NAT and network policy of access list of the network security appliances. The network security appliances will translate and accept the configured IP addresses of the workstation or server to access the connected common area network to share the resources.

TABLE I. NAT TABLE OF UNIVERSITY HOSPITAL'S FIREWALLS

Sources for NAT	**NAT Table of the Hospital University**		
	Source Workstation's Internal IP Address	***NAT Firewall's Internal IP Address***	***NAT Workstation's External IP Address***
Workstation 1	Subnet-A-IP-2	Subnet-A-IP-1	Subnet-B-IP-1
Workstation 2	Subnet-A-IP-3		
Workstation 3	Subnet-A-IP-4		

TABLE II. NAT TABLE OF GOVERNMENT HOSPITAL'S FIREWALLS

Sources for NAT	**NAT Table of the Government University**		
	Source Server's Internal IP Address	***NAT Firewall's Internal IP Address***	***NAT Server's External IP Address***
Server1	Subnet-C-IP-2	Subnet-C-IP-1	Subnet-B-IP-2

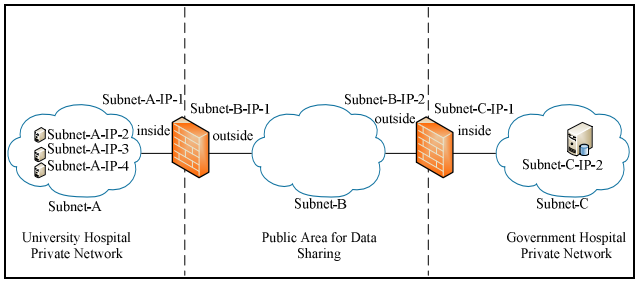

Figure 1 Network Infrastructure of Healthcare Entities

REFERENCES

[1] Yang Yang, Hu Bing, "Analysis on Construction Work of Hospital Network Security," China Digital Medicine.-2010, 5(12): 97-98

[2] Gong Yan-ting, Chang Jian-guo, "Application of VLAN Technology in Deployment of Hospital VLAN," Chinese Medical Equipment Journal, 2009, 30(3): 43-45, 48

[3] Li Xiang, Tang Hui, "Application of NAT Connection Between Configuration Hospital and Medicare Data Center," Chinese Medical Equipment Journal, 2009, 30(11):46-47

[4] Cisco NAT Website, Information about NAT, http://www.cisco.com/en/US/docs/security/asa/asa83/configuration/guide/nat_overview.html, last access on 11th, Feb, 2012.