

Hillstone Networks Successful Case

—Beijing RedBaby Information Technology Co., Ltd

Customer: Beijing RedBaby Information Technology Co., Ltd.

Industry: Enterprise

Customer Requirements: Efficiently manage and control Internet applications, VPN function, attack defense, security network with QoS function, security transfer of business data between headquarters and branch offices, security transfer of OA and mail

Platform: Hillstone SG-6000-G5150、Hillstone SG-6000-G2120、Hillstone SG-6000-M3100

Provided Functions:NAT/firewall, IPSec PVN, security defense (including ARP defense), QoS

Customer Introduction:

Beijing RedBaby Information Technology Co., Ltd., established in March, 2004, is a leading catalog and web B2C enterprise, providing fast convenient purchasing method for customers at lower cost. After years of development, RedBaby has established the operation with catalog and Web site as the channel, and integrated marketing center, purchasing center and operating center as a system. Beijing RedBaby Information Technology Co., Ltd. has 15 subsidiaries located at Beijing, Shanghai, Tianjin, Wuhan, Guangzhou, Ningbo, Shenyang, Chengdu, Suzhou, Nanjing, Wuxi, Dalian, Xi'an, Shenzhen and Hangzhou.

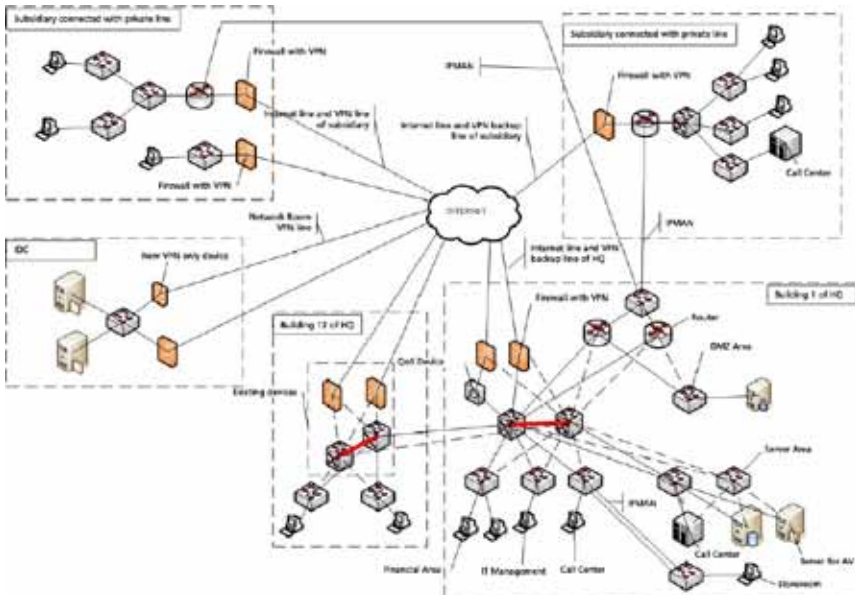
Current network situation of Beijing RedBaby Information Technology Co., Ltd.

Network of Beijing RedBaby Information Technology Co., Ltd. is categorized into three classes: the first class is the network of headquarter, the second class is the network of subsidiaries, and the third class is the network of deliver center. The ERP system is used to transfer data between headquarters, subsidiaries and delivery centers. E-commercial businesses, such as ERP, FTP, Mail, etc, are running in the enterprise network. The core network of Building 1 and Building 12 of the headquarter are interconnected and act as backup of each other. Servers of the company are IDC hosting.

The main security concern of the customer is as follows:

1. Some of the devices experienced of illegal intrusion, network penetration, DoS/DDoS, etc.
2. Traffic bandwidth are sometimes taken up by the personal use of online video, P2P downloading, which seriously impacts the running of normal business application.
3. IPsec VPN should be used between headquarters and subsidiaries, keeping sensitive data safe.
4. Networks of Building 1 and Building 12 in headquarters are used for daily office work, and all network orders are processed in the headquarter. Devices should be deployed with redundancy, guaranteeing a non-stop operation of the network.
5. Take into account of the future development of the network, the performance should be extensible, protecting the initial investment.

As shown in the network diagram, in order to protect the DCN Intranet effectively, Jiangsu Telecom uses a dual layer defense architecture. In the first layer, firewall function on the Cisco 6509 was turned on to filter inbound and outbound traffic. In the second layer, two Hillstone SA-5040 devices are deployed, forming a security filtering area to protect DCN Intranet.



Solution characters of Beijing RedBaby Information Technology Co., Ltd.

After evaluation and comparison, considering qualification, technical strength, service level, product functionalities, performance, and product's price vs performance, Beijing RedBaby Information Technology Co., Ltd. chose Hillstone Networks' professional solution. Building 1 selected SG-6000-G5150, Building 12 selected SG-6000-G2120, and subsidiaries selected SG-6000-G2120 or SG-6000-M3100 depending on network sizes.

According to customer's requirements, G5150s of Building 1 and G2120s of building 12 are deployed in Active-Passive mode. Depending on network sizes, G2120 or M3100 are deployed at subsidiaries. NAT function is used on the devices for Internet access and access to servers in IDC room. Security defense is turned on to avoid attacks from both internal and external network. QoS is configured to control P2P and video applications. IPSec VPN between headquarters and subsidiaries ensures encrypted data transfer. The third generation SSL VPN provides reliable user authentication and data security for subsidiaries and delivery centers.

- **Robust and high-effective processing capability**

Hillstone SG series new generation multi-core security appliance is based on multi-core Plus G2 architecture. The application processing performance is greatly improved. This architecture provides a professional and high-performance hardware platform for enterprise application security, guarantees much higher, more reliable, more stable and more secure integrated processing capability. The improved performance satisfies customer's requirements, and ensures that the devices are not bottlenecks in the network.

- **Professional firewall function**

Hillstone SG series has a professional firewall function module. Through configuring related firewall policy rules, interzone policy control is realized. The user control is precise and fine grained, guaranteeing data safety on the firewall layer. In the mean time, the tight control of security policy rule effectively resolves the hidden problems between Intranet and access layer, ensuring security at network boundary. Rich NAT functionalities provided by the appliance make it possible for hundreds of PCs to access the Internet through limited public IP addresses, protecting the topology of Intranet.

- **High-performance IPSec VPN and SSL VPN**

Hillstone SG series IPSec and SSL VPN provide a perfect solution for communication between headquarters/subsidiaries/delivery centers, and remote access by employees on business trip or work from home. No matter which access method (IPSec VPN or SSL VPN) is used, VPN users can access related resources on the intranet easily, flexibly and effectively, with safety ensured, providing fast user access, data transfer and internal resource access.

- **High attack defense capability**

Hillstone SG series offers a set of ARP defense solution: authentication based ARP exchange between client and appliance, static binding of IP and MAC, static binding of MAC and port, ARP learning, and automatic sending of gratuitous ARP packet. All of the above are useful and effective to control intranet ARP attack.

Hillstone SG series integrated SYN Proxy, SYN-Cookie, UDP filter, ICMP filter, and session control. With zone based control, the follow attacks can be defended: SYN flood, ICMP flood, UDP flood, Ping of Death, Teardrop etc.

In this project, the combination of ARP defense and attack defense together with session control capability provide a comprehensive defense while guaranteeing connectivity, offering customer a green and healthy network system.

- **Flexible bandwidth control**

Formerly, the network of the customer is filled with BT, Xunlei, eMule, etc. With the flexible bandwidth control function that Hillstone SG series offers, the following QoS policy is configured: set bandwidth limitation to each IP and allocating precise bandwidth to several kinds of applications; limiting the maximum bandwidth of P2P downloading and online video; guaranteeing the highest priority for key business applications.

With the monitor and log functions, Hillstone SG series offers detailed network traffic analysis report to the IT department, allowing administrator to understand and control network usage and activity. It also provides intuitive and reliable basis for network management. With the help of schedule functionality, customer can monitor and manage network traffic effectively at real time, allocating bandwidth flexibly, guaranteeing non-stop operation of key business application, greatly improve the bandwidth utilization.

- **Effective AV**

Before the security appliance was deployed, virus outbreaks often brought the network down. Hillstone SG series high-performance AV function provided first layer AV defense for the whole intranet. The parallel stream based AV engine takes full advantages of multi-core Plus G2 hardware architecture, ensuring high AV performance and low latency when traffic is passing through the appliance, so that user' s experience is not affected.

- **Strong session control function**

According to different situations of different network segments, session control is implemented to control session numbers for source IPs and destination IPs. Service quality is improved on the Internet link, the limited NAT port problem is resolved, and the bandwidth utilization is improved.

Commends from customer

Hillstone SG series new generation security appliance offer us fine grained security control, and the attack defense function resolves the problem of frequent attacks and unstable network. In addition, Hillstone SG series effectively control the traffic of business and personal applications, and the special monitor function gives a clear view of the bandwidth usage situation on the network. The VPN function resolves the data transfer and security authentication problem among headquarters, subsidiaries and delivery centers. To summarize, Hillstone Networks' solution speeds up our information security construction, meets our requirements in all aspects, including performance, functionalities, and services. The solution provides a healthy network environment, and brings us better user experience in network and applications.