



Hillstone Network Security Solution for Telecom Industry

1. Overview of Telecom Network

China's telecom industry has been developing rapidly in recent years. The country's total internet subscribers exceeded 600 million, at an average annual growth rate of 42% in the last four years. Fixed telephone subscribers have increased 16 times, mobile subscribers have increased 400 times, creating a miracle in the world telecommunication development history.

China took many reform measure in the telecom industry, such as the carrier partitioning, which creates favorable conditions for competition from multiple telecom carriers. In order to achieve success in harsh marketing environment, it requires each telecom carrier to provide efficient, high quality services. To provide around the clock uninterrupted services, telecom carriers puts strong emphasis on the security and reliability of telecom systems.

The security issue has become a serious problem of telecom industry in recent years, especially for the rapid developing Internet service and telecom value-added services. Telecom value-added services are the main growth engine of telecom industry, which injected new vitality into the development of telecom industry. Traditional telecom carriers and mobile telecom carriers provide various value-added services based on IP data, such as fixed-line broadband operation, dedicated line, broadband storage, server co-location, multimedia, VoIP, video etc. Carriers are experiencing explosive revenue growth in these areas. However, how to reduce operating cost and increase operating revenue in the more intensely competitive market is becoming a particularly urgent problem. In order to seize these opportunities and challenges, telecom carriers must build an effective application service network structure, and the security control of network and application services is the key to business success. Various security threats may bring great damage to telecom companies, and system with incomplete safety protection will lead to problems such as decline in operating revenue, rise in maintenance cost, and reduce in customer loyalty.



Hillstone Network Security Solution for Telecom Industry

2. Analysis of Challenges Generally Faced by Telecom Industry

These are the information security problems and challenges faced by telecom carriers today:

1、Application Security of Internal Telecom Business

Focus Areas: Security zone separation, SSL VPN remote access, insider attack, traffic optimization, as well as virus and application layer security protection.

The DCN network of China Telecom is in charge of supporting internal Telecom business traffic. It is usually divided into four major parts, OA, BOSS, Accounting, and other business. The DCN network are facing the following critical problems: separation of different business, bandwidth guarantee for key business applications, security zone separation of different business units and security levels of users, and attack defense to both external and internal threats, among which ARP attack is the most prevalent.

2、Telecom IDC Application Security

Focus Areas: Access control, network layer attack defense, application layer intrusion prevention, bursty traffic, and traffic load balance.

In recent years, one developing trend is that IDC is becoming more and more important for enterprise IT. Large amounts of data and business are concentrated in IDC, which in turn leads to the rapid growth of IDC networks. With IDC now as the core of the fast-developing Internet industry, security issue is becoming a very serious problem for IDC. This poses an unprecedented challenge to the security and processing capacity of security devices at IDC network edge.

Problems currently faced by IDC users are summarized as follows:

- 1、 Traditional security device have insufficient performance, particularly in new connection setup performance and small packet processing capacity cannot meet the demand of increasing traffic.
- 2、 Lack of effective attack defense ability (including attack from network layer and application layer).
- 3、 Lack of effective traffic management function, cannot effectively protect the IDC server when attack and abnormal traffic appears.
- 4、 Lack of traffic load balancing function.



Hillstone Network Security Solution for Telecom Industry

3、 DNS Server Anti-DDoS Attack

The “5.19” event which led to Internet disruption lasted over 24 hours in more than 20 provinces of the nation. It sounded the alarm for telecom carriers and third-party providers. For DNS servers serving for the entire Internet, how to prevent attacks and maintain normal operation under heavy traffic pressure has drawn wide attention.

4、 Network behavior control of broadband service

As telecom carriers easily have tens of thousands of customers, problems such as user authentication, management, accounting, and auditing needs to be resolved.

On the one hand, security threats from both inside and outside the network are quite serious. Some of the internet users are nonprofessional users, with systems that may contain various application software infected with virus. These people may not have enough security and network expertise. Their systems may become springboards for attacks. The application of the customer (P2P traffic, online video, number of sessions) needs to be monitored to help manage their network usage.

On the other hand, it is necessary to provide strict controlling and auditing of user actions such as browsing inappropriate web sites, making inappropriate posts through email, BBS, chatting room, and IM, and even engaging in illegal activities.

5.Needs for high-performance and high-reliability security appliance

Today’ s Internet traffic pattern is gradually changing. Percentage of small packets are increasing, concurrent connections of single user are increasing, and UDP packets are increase rapidly. On another hand, traffic bandwidth and security functions are also increasing, putting higher and higher requirements on processing performance of security appliance.

Carriers expect to maintain the long-term stability and availability of network in a high-security environment.

3、 Hillstone Networks Network Optimization Solution

1、 Security enhancement of DCN network

Hillstone Networks security appliance addressed various security problems in DCN network with its high performance and richsecurity functions.

- Hillstone Networks provides various operating modes such as route mode, NAT mode, transparent mode and mixed mode, in options such as HA and bypass, which



Hillstone Network Security Solution for Telecom Industry

can meet various deployment scenarios and guarantee the stability and reliability of the network.

- Security zone definition and policy control by stateful inspection.
- Bandwidth management and session control based on IP and application protocols.
- ARP attack defense.
- Network behavior monitor, control and audit.
- High performance in session rampup per second and large-capacity of concurrent connections to guarantee normal network operation and resist network layer attacks.
- Hillstone Anti-Virus supports virus scanning of HTTP, FTP and multiple Email protocols to reduce security threats.
- Hillstone IPS offers effective application layer attack defense to protect the security of the business and data server.

2、IDC application security

- Session rampup per second and large-capacity concurrent connection to guarantee normal network operation and resist network layer attacks.
- Hillstone Anti-Virus supports virus scanning of HTTP, FTP and multiple Email protocols to reduce security threats.
- Hillstone IPS offers effective application layer attack defense to protect the security of the business and data server.
- Hillstone supports HA, AA, and bypass card to offer high-reliability for all kinds of deployment environment.
- Third-generation SSL VPN technology – Hillstone Secure Connect provides convenient remote access.
- The virtual system technology provides virtualization of one devices into multiple virtual firewalls.

3、DNS security protection solution

Due to the hardware architecture limitation, most traditional security devices are not deployed inline when protecting DNS, web sites and application services. This mode not only has many limitations including inability of blocking bad traffic in real time. With Multi-core Plus® G2 architecture and 64-bit parallel processing system, Hillstone Networks security appliance has strong packet processing capability as well as attack identification and prevention capability. The multi-core architecture has more robust and stable performance when compared to traditional x86 and ASIC. Hillstone security



Hillstone Network Security Solution for Telecom Industry

appliance has been successfully deployed in front of DNS servers of many provincial level telecom carriers. The appliance not only can block network attacks, but also reduce burden on DNS servers, effectively improving the service quality of carriers.

4、 Network behavior control

Hillstone Networks security appliance provides unified management of user authentication, accounting, auditing, and behavior control for telecom carriers. With Hillstone Networks security appliance as the security access device, user can be identified through L2TP and Web authentication. Network resource allocation can be performed based on the identity of users. Administrators could manage the bandwidth allocation based on users' package.

- Outbound Message Control: control and audit of webpage browsed, outbound email, and BBS posting.
- URL Filtering: Predefined and user defined URL categories for control of website based on category.
- Log Auditing: Record user' s network behavior, such as online game, instant messenger, online stock transaction, FTP/HTTP, P2P download, online video, web browsing, email, content and attachment, BBS posting, etc.
- Provides pluggable hardware storage module

5、 Provide high-performance and high-reliability security appliance

Carrier networks have large number of users, heavy traffic, long period of sustained peak. With multi-core architecture and 64-bit security operation system, Hillstone Networks security appliance offers multi-function, high-performance solution for carrier network needs. Household customers usually access internet at several fixed periods. And there will be tens of thousands of network requests per second at these periods. Hillstone Networks security appliance can support up to hundreds of thousands of session rampup per second, meeting the demand of concentrated access requests form clients at network peak times. With many years of carrier-grade hardware innovation experience, Hillstone Networks security appliance also maintain network stability by adopting high-reliable hardware design and series of software functions such as self-monitoring alarm and HA.

6、 Provide high extensibility, protect carrier investment

Some models of Hillstone Networks security appliance have modularized design.



Hillstone Network Security Solution for Telecom Industry

Currently, three kinds of pluggable hardware modules are available: interface module, application processing module and storage module. The modularized design can extend the interface, performance, and storage capacity of the appliance, greatly protecting customer' s investment. Interface modules enhance the connectivity of the device; application processing modules increase the security processing capability of the appliance; and storage modules can timely store logs and statistics collected by the device.