

Firewall

Firewall is a set that protects and separates inner private network from Internet, it can filter packets according to information of source address, destination address, port and packet state that contained in IP packets transmitted on network, and control whether the packets pass or not.

Firewall becomes a popular method to control visit to network. This is a usually used and effective method to keep away hackers. To any pivotal server, it is suggested to set behind firewall.

Firewall can be router, personal host computer, main system or a serial of main system. And it specially separated network or subnet from outside. Firewall system always locates on high level gateway such as Internet connecting point, but it can also locate on lower level gateway so that it can protect some low-quantity main system or subnets.

1 Advantages of adopting firewall

Firewall can improve security of host computer and subnet, the main advantages of Asianux firewall system are:

- Ensure safe visit to host and applications
- Ensure security of several clients and server
- Protect pivotal department from inner or outer attacking, provide safe channels for employee, client and provider that pass Internet and visit long-distance computer.

2 Basic principle of safely controlling of firewall

Security strategy is the spirit and basic of firewall. Before set up firewall, it needs to put forward a perfect whole security strategy based on security status quo, risk evaluation and commercial requirement. This is the key of configuring firewall. There two basic rules on security control of firewall:

- Allow all visits except definitely denied visit ---- all not denied visit are allowed
- Deny all visits except definitely allowed visit ---- all not allowed visit are denied

We can see that, the later one limit more.

3 Basic type of firewall

There has many types of firewall, and generally these can be classified to two classes: one is based on packet filter; the other is based on proxy service. The difference between them is Firewall that is based on packet filter usually transmit messages directly, it is absolutely transparent to user and has high speed. But Firewall that is based on proxy sets up connection through proxy service, it can have more strong identity validating and registering function.

- Packet filter firewall

Packet filter is that selectively pass data packet on network layer, examine every data packet in data stream according to the filter logic that set by system, confirm whether to allow this data packet to pass according to its source address, destination address and port. Packet filter firewall will examine all IP addresses that pass information packet, and filter information packet according to filter rule given by administrator. If firewall set one IP to be dangerous, all information that come from this address will be shielded by firewall.

Packet filter is usually installed on router, of course, the PC that used as router also can be installed with Packet filter, and it may have more powerful functions, such as iptables in Asianux 2.0.

IP address and port number are the characteristics of network layer and transmitting layer, but Packet filter can also work on application layer. Applications on Internet usually have special port number. For example, telnet service always runs on port 23 of TCP. So, we can set a Firewall to prevent from sending telnet request to inner nodes.

The advantage of using Packet filter Firewall is that it can implement firewall function almost without adding any additional fee on quondam network, because that almost all routers can filter packets pass by. Currently, 80% of installed Firewalls are Packet filter mode, they all set filter principle on router that connects inner network and Internet.

Packet filter Firewall needs no username and password, user may not feel it. This kind of Firewall has high speed and is easy to maintain. It has better network capability and clarity of application. Of course, it can not effectively distinguish different users that have same IP address, so its security is relatively lower.

- Proxy Server

Proxy server is also called application level server. Proxy service means that connection between application layers of computer system in and out of firewall is implemented through two connections that stop at proxy service. This way, it successfully separates computer systems in and out of firewall.

Application-level gateway uses software to transmit and filter especial applying service, such as connections of TELNET and FTP service. This is proxy service. It only allows service that has proxy to pass; that is to say, only services that are considered to be “reliable” are allowed to pass firewall. Additionally, proxy service also can filter protocol, such as filter connection, deny to use FTP laying command etc. Application-level gateway has function of enrolling, dairy, statistic and report. And it also has good auditing function, can have strict user validating function.

Proxy server always has high-speed cache; it can save time and resource. Proxy service has advantages of information converting, effective validating and logging, simplifying filter principle. Network Address Translation (NAT) service can shield inner IP addresses of network, and make network frame to be sightless to outside.