Efficient Firewall Architectures over Label Switching Network

Satoshi Uda

School of Information Science,
Japan Advanced Institute of Science and Technology

February 15, 1999

Keywords: Internet, label switching, firewall, security, packet filtering.

The Internet consists of the interconnections of many routers. A router must perform complicated IP processing (i.e., looking up the complex IP routing table, e.t.c.) for every packet, in order to perform packet forwarding in the 3rd-layer (Network-layer). The number of the Internet users increases abruptly and the number of the applications which requires broad band and low delay also increases. In such a situation, mass data must be process at high speed in a router. The method using label switching technology has been proposed as one of the method to resolve this problem.

A "label" is attached to the packet which flows inside a label switching network. In a label switch router (LSR), the packet to which the label has been attached is transmitted by the 2nd-layer switch without the 3rd-layer intervention. In this state called cut-thru state, high-speed processing of mass data is realized because there is no 3rd-layer intervention.

Further more, it has been crucial problem to protect a user's information and resources from the exterior owing to the expansion of the Internet. The way of firewall is used frequently to resolve the solution. In building firewall, the packet filtering function provided a router plays an important role. In the router which provide packet-filtering function, the information on the 3rd or more upper layer must be picked up, this information must be evaluated, and forwarding must be controlled according to the evaluation result.

The firewall technology is needed also over the label switching network which realizes broad band and low delay. However, over the label switching network, it is difficult to pick up the information on the 3rd or more upper layer and control forwarding, which are needed for a packet filtering function, owing to the characteristic that a packet is forwarded in the 2nd-layer.

Then, in this paper, I propose the following two mechanisms. These mechanisms don't conflict the advantage of lavel switching network.

- **The mechanism using virtual cut-thru**

  The packet forwarding module (PFM) which operates in the 2nd layer is added to LSR which provides a packet-filtering function. PFM applies filtering rules to input datagram, and if forwarding is accepted as a result, it will output datagram.

  LSR generates the "virtual cut-thru path" which bypasses to PFM, instead of generating a normal cut-thru path at the time of generation of a cut-thru path. By this, all the datagram in a cut-thru state will be forwarded through PFM. This mechanism is realizable by change of only LSR which provides packet-filtering function. In the packet forwarding process in the 3rd-layer, IP processing (i.e., looking up the complex IP routing table, e.t.c.), not originally needed for filtering process, also needs to be performed. However, in PFM, since transmission by the 2nd-layer is performed, the high-speed forwarding which short-circuited these processes is possible.

- **The mechanism to entrust filtering function to the LSR at an end of the cut-thru path**

  Over a label switching network, packet forwarding in the 3rd-layer is performed at the end of a cut-thru path also in the cut-thru state. This mechanism entrusts packet-filtering function to the LSR at an end of a cut-thru path.

  About the path which succeeded to entrust, normal cut-thru becomes possible. Within the cut-thru path, the datagram can forward without any reassembling and evaluation of a packet. This is in the ideal state for a label switching network.

Perfect cut-thru is possible by using the mechanism to entrust filtering function to the LSR at an end of the cut-thru path. This is the most ideal mechanism. However, it is required that many LSRs are made to correspond to this mechanism and the maintenance of a security level based on management suitable for the all. it is very difficult.

Therefore the method of combining PFM mechanism and function entrusting mechanism is realistic. By combining PFM mechanism and function entrusting mechanism, packet filtering which makes the best use of the feature of a label switching network is realizable. As a result, the best firewall mechanism over label switching network is realizable.

Moreover it considers as the function to process by using the information on a packet on LSR besides packet filtering, and NAT function and the replacement function of a label are mentioned. It is easy for the technique proposed in this paper to apply to these functions.

I premised on using a label switching network in this research. A future subject is loosening this restriction and examining the extension to the distributed firewall building technique in a general network, on the basis of the proposal in this paper.