Advances in Computer Science Research (ACSR), volume 61
7th International Conference on Education, Management, Computer and Society (EMCS 2017)

Embedded Firewall Based on Data Driven Technology

Wenjun Su[1, a*] and Haitao Chen[1, b]

[1]Department of Electronic Information, Guangzhou Civil Aviation College, Guangzhou 510000, China

[a]suwenjun@139.com, [b]chenhaitao@caac.net

Keywords: Stateful packet inspection; Embedded firewall; Data driven; Self-time pipeline

Abstract. The traditional network perimeter firewalls can not pre-vent internal attacks, and performance and security of personal software firewall are poor. In view of this, we design and implement an embedded data-driven hard-ware firewall. Implemented with stateful packet inspec-tion, the proposal firewall has higher performance and security. Data-driven processor provides us natural mul-tiprocessing capability without any process scheduling or complex interrupt handling, and power savings. Em-bedded data-driven hardware firewall is robust, secure, and has low power consumption and high performance. Moreover, the firewall can detect and prevent new at-tacks. Experimental results show that the firewall can meet Gigabit Ethernet IP packet processing.

Introduction

The traditional edge firewall can only guard against the external attack to the enterprise network, and provides protection to the periphery. These firewalls will filter and review the data flow from the external Internet into the enterprise intranet. However, edge firewall cannot guarantee the security of Intranet Security access. For example, a hacker can use the computer to invade other computer and system of network, when the control right of this computer is acquired.

The latest security solution is to distribute the firewall function to every computer and server in the network. Embedded firewall can extend the security access to the network, and solve the problem that the edge firewall can't prevent the network attack. Security measures are implemented in the terminal, which is implemented by the hardware system of the Embedded Firewall, and independent of the computer operating system. This program can make the enterprise network is not subject to external or internal threats of any hacker attacks and malicious code.

Structure of Embedded Data Driven firewall

Introduce to Data Driven Processor DDMP. DDMP (Flow Multimedia Processor Date) is a data driven processor developed by the Sharp Co, with 0.25 micron technology and the performance of 8600MOPS. DDMP uses the self-timed pipeline, which is different from the traditional synchronous clock pipeline. A four phase handshake protocol is used to control the com-munication between the self-timed flow line segments. The throughput of the pipeline can be changed, and dif-ferent segments can have different delay.

Due to the use of data driven and self-timed pipeline design, DDMP has low power consumption, high paral-lelism, there is no clock skew and the average perfor-mance instead of the worst performance, natural pro-gramming language advantage.

Structure of Embedded Data Driven Firewall. In order to make the embedded firewall can handle high-speed data streams. In this paper, efficient hard-ware platform and parallel pipelining algorithm to achieve the above function module is used, and the final target is implementation of small volume, low power consumption and High Performance Embedded Firewall, which can be embedded into the CF card or mobile phone.

The data dependence of the modules in the Embedded Firewall is shown in figure 1. If these data flows run in the DDMP chip, it can be used to make use of the ad-vantages of DDMP. That is to say, the data flow dia-gram in Figure 1 is the key point of the data driven firewall system:

(a) Efficient dynamic multiple processing (including process creation, execution, and deletion).

(b) Parallel implementation of all filter module (includ-ing classifier, packet monitor SPI and application layer filter APF).

(c) High speed packet buffering mechanism, and has access to the chip memory (such as DDR-RAM, SDRAM) module.

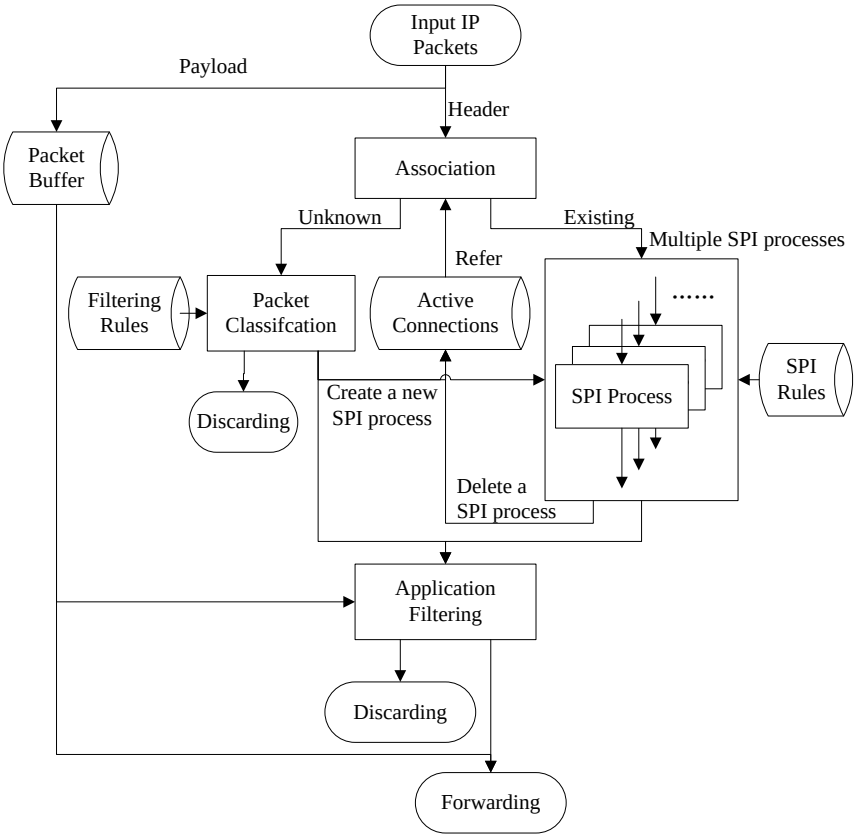

Figure 1. Basic data flow of Embedded Firewall System

Realization of Embedded Data Driven Fire-Wall

Ip Packet State Detection. The state detection firewall is firstly proposed by Point Check, also known as the dynamic packet filter firewall. State detection is a technology that tracks the detection of the connection from the TCP to the termination of the whole process, maintains a dynamic state information table and checks the subsequent data packets. The only drawback of the state detection firewall is that this state detection may cause a delay in the network connection, but the faster the hardware, the more difficult to detect the problem.

(1) Monitoring state change

In the state detection of TCP, we only care about the establishment and the end of the TCP connection. the establishment and the end of the TCP connection can be simplified to figure 2. Embedded hardware firewall based on Figure 2 for TCP session state change detec-tion.

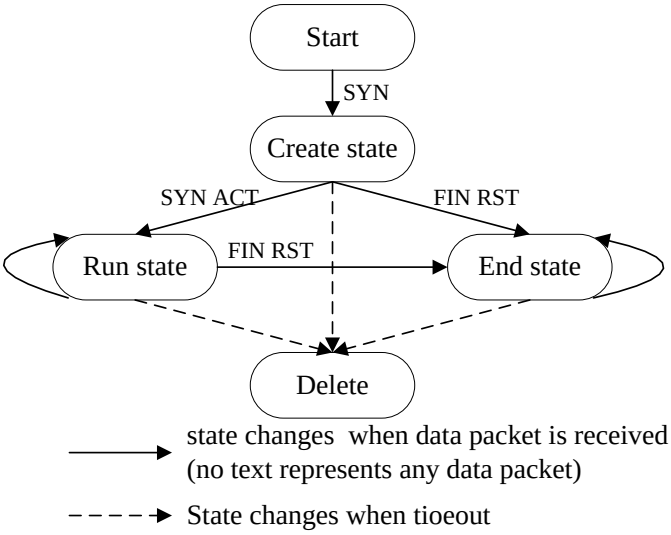

Figure 2. TCP connection state transition in the state detection table

Although the UDP connection is stateless, it still can be maintained in a similar way, and virtual state is used to detect. When UDP data packets go through the firewall, this session is added to the state detection in the table and set a timeout value. Packet will be allowed to pass through within the time, and packet will be discarded when timeout. The change of UDP session state detec-tion is shown in figure 3.

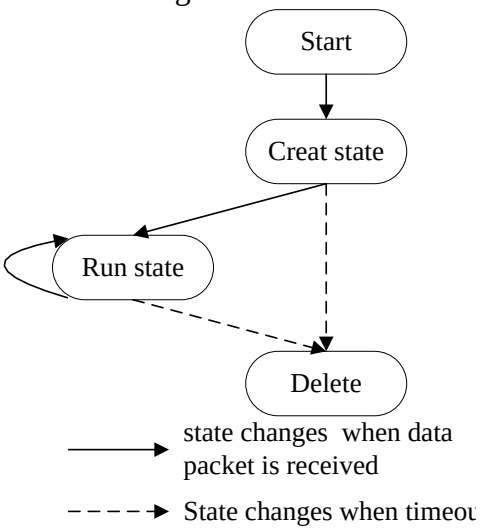

Figure 3. TCP connection state transition in the state detection table

State inspection firewall system can realize the general function of the filter, and obtain the status information of the transport layer and the related information of the application layer. Filter achieves safe filtering according to these information and user defined security policy after the information has been analysed.

For a simple example, packet filtering technology can-not stop flood attack of SYN packet, but state detection technology can easily cope with. When the server sends back a SYN + ACK packet, the firewall can determine that the server is waiting for response. And then the firewall pre sends an ACK package to the server and start the timer. If ACK packet of the client dose not re-ceived within the time, then a signal will be sent to reset the server for waiting for the next connection.

(2) Data structure and management of the state monitor-ing table

When condition monitoring, confirmation for a session can be distinguished by using the destination address, source address and port number, and the maintenance for the sequence number of the TCP connection should be considered. In Embedded Firewall, because the local IP address is determined, the session can be distin-guished only by remote IP address, remote and local port number. Before IP data packet is processed, the destination IP address field is changed to the local IP address, and the source

port is changed to the remote port, and destination port is changed to the local port. Thus, the IP data packets are processed in a unified way.

The data structure of the hash table and tow-way linked list is used as the storage state detection table shown in Figure 7. Hash table lookup time complexity is O(1), and two-way linked list is conducive to the realization of the table add and remove operations which time complexity is also O(1). The Hash table stores the ad-dress of the first table, and the state detection table en-tries are indexed by the remote IP address as the index distribution in the hash table. Because the remote IP address is uniform, the distribution of the hash table is also uniform. Using a linked list allows the storage space to make full use, and the distribution of storage space use IP address as the index. For example, in the design of the implementation of the table space is 128, the low 5bit of the IP address is used as the index to find and allocate the remaining space. Thus, the time of finding the remaining space is greatly reduced com-pared to the linear search method.

For the search optimization, a hybrid method of soft-ware hash table and small capacity CAM can be used to realize associative memory. Preliminary experimental results also show that, compared with no CAM software implementation method, this scheme can reduce the search time of 30% - 90%.

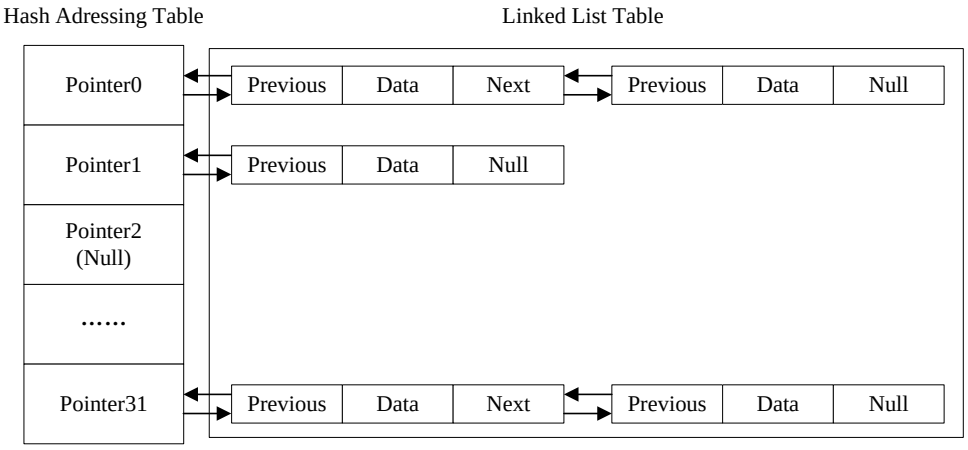

Figure 4. The data structure of hash table and tow-way linked list

Packet Filtering. The LC trie tree algorithm is used for packet filter. LC Trie tree is a data structure that is suitable for the long-est prefix matching. The general tree structure depth is O (log N), where N is the number of entries. This shows that the number of memory accesses in general tree structure increases with the increase of the number of entries. When there are a large number of entries, the search time will continue to grow. On the other hand, the depth of the LC trie tree is lower than that of the two fork tree, which depth is O (log log N). Thus, for the IPV4 address, the depth of LC trie tree is about 5, and the average memory access times of up to 5 times. Moreover, the LC trie tree is easy to extend to the IPV6's long address. Therefore, LC trie tree is used as the basic data structure of the packet filter.

Application Layer Filter. In the program, head of IP packet is examined to deter-mine whether the IP package is TCP package. If this is a TCP package, the firewall will check the contents of the IP package, and determine whether this is the HTTP request packet.. URL filtering rules are used for URL filtering.

Firewall Performance Testing

The function and performance of the firewall are tested by simulating the TCP packet flow. In this paper, the simulation software DVW (Visual Workbench Data-driven) and the actual chip are used for test and compar-ison.

Stateful Packet Inspection (SPI) Module Test-Ing. The function of the SPI module is mainly including the search for the status detection table and status pro-cessing of the table list. The throughput

of multiple connections through the SPI module is tested using the number of connections to be 16, which represents the maximum network traffic that can be handled by a fire-wall.

Table 1 is the test result. From the test results, the per-formance of the actual chip is better than that in the simulation environment DVW. The test results of the chip are based on the actual test results.

Table 1. Test result of SPI module

Type of IP packet	Thoughput
GET packet	6.5kpps
Non-GET packet	1.08Mpps

Line speed is: 4.3Mpps×54Byte/IP ×8bit/Byte = 1.86Gbps, where the smallest IP packet in the local area network is 54Byte. Using average packet length that is 536 bytes, the average throughput is: 4.3Mpps×536 Byte/IP×8bit/Byte = 18.4Gbps.

This is more than sufficient throughput for the applica-tion of Gigabit Ethernet, or even to meet the enterprise application. Of course, this is just the throughput of the SPI module and there are other modules that need to take up processor resources.

URL Filter Module Testing. The performance of the module is related to the IP packet type and the parameters that are the length of the URL, position of the URL string in IP package and the stored sequence number matching with the URL rules.

The tests results show that the offset of the URL string in the TCP data package of relatively large impact on throughput, and directory name length and the stored sequence number matching with the URL rules have little impact on the throughput.

If the HTTP package does not contain "GET" command that means the package does not contain the host and directory name information. Then, the HTTP package does not require URL filter. At this time, the processing speed is greatly improved. Test results are as follows:

Table 2. Test result of URL filter module

Throughput in DVW	Throughput in chip
2380kpps	4300kpps

If the average length of the TCP packet is 536 bytes, the average throughput is 1.08Mpps×536 Byte/IP× 8bit/Byte = 4.63Gbps. In HTTP applications, most of the IP packages are non-GET package, and the speed is enough for HTTP personal applications.

Conclusion

Through the test, the ability of the SPI module in the Embedded Firewall can meet the needs of the Gigabit Ethernet. DDMP can handle multiple connections in parallel, which is suitable for network processing.

In this paper, the Embedded Firewall Based on data driven is implemented and the performance test is car-ried out. Fortunately, the ideas have been verified that data driven processor can be used for firewall and other network applications. IP packets in a data-driven pro-cessor are high-speed parallel processing, and the fire-wall can meet the current network performance re-quirements.

References

[1] John A. Sharp. Data Flow Comupting: Theory and Practice[M]. New Jersey: Ablex Publishing, 1992

[2] Hiroaki Terada, Souichi Miyata, and Makoto Iwata. DDMPs: self-timed super-pipelined data-driven multimedia processors[J]. Proceedings of the IEEE, 1999,Vol 87, No.2: 282-298

[3] Burrus C S. Index Mappings for Multidimensional Formulation of the DFT and Convolution[J]. IEEE Trans on A SSP, 1977, 25 (6) : 239～ 242

[4] Andrew P. Moore, Robert J.Ellison, Richard C. Linger. Attack Modeling for Information Security and Survivability[J]. USA: Software Engineering Institute, Carmegie Mellon University, 2001: 3~26

[5] Tomas A. Longstaff, James T. Ellis, Shawn V. Herman, et al. Security of the Internet[J]. USA: Software Engineering Institute, Carmegie Mellon University, 1998: 5～12

[6] D. Morikawa, T. Matsumoto, and M. Iwata. Fast Packet Filtering in Data-Driven Embedded Firewall[C]. NEINE'04, Sep. 2004