Settings firewalls to implement special filtering mode
Gulomov Sh.[1], Nuriddinova M.[2], Nuruddinova A.[3] (Republic of Uzbekistan)

Настройка межсетевых экранов для реализации режима специальной фильтрации
Гуломов Ш. Р.[1], Нуриддинова М. Ш.[2], Нуруддинова А. Г.[3]
(Республика Узбекистан)

[1]Гуломов Шерзод Ражабоевич / Gulomov Sherzod - ассистент,
кафедра информационной безопасности;
[2]Нуриддинова Мохинабону Шахобиддин кизи / Nuriddinova Mokhinabonu – студент,
направление: информационная безопасность,
Ташкентский университет информационных технологий;
[3]Нуруддинова Адиба Газиевна / Nuruddinova Adiba - кандидат экономических наук, доцент,
кафедра экономики труда и управления,
Российский экономический университет им. Г. В. Плеханова,
(Ташкентский филиал), г. Ташкент, Республика Узбекистан

Abstract: *this article describes the structure of the packet Ethernet, which determine the type of protocols and standards of the network traffics. Developed a method for calculating the invariant characteristics of traffics for a special filtering mode with two physical interfaces and parametric conditions of implement the special filtering mode through virtual connections. Offered a model of a virtual TCP connection to the physical network, allowing ensure H (exponent Hurst) to input and output Firewall and performing the estimate of the accuracy of a special filtering for defining the intensity of the packet and performance of Firewall and also analyzed conditions of implementation of the Firewalls in special filtering mode.*

Аннотация: *в данной статье рассмотрена структура пакета Ethernet, определяющий тип протокола и стандарта сетевого трафика. Разработан способ расчета инвариантной характеристики трафика для режима специальной фильтрации с двумя физическими интерфейсами и параметрические условия реализации режима специальной фильтрации через виртуальные соединения. Предложена модель виртуального TCP соединения на физическую сеть, позволяющая обеспечить неизменность H (показатель Хэрста) на входе и выходе межсетевого экрана и способ оценки точности выполнения режима специальной фильтрации при определения интенсивности пакета и производительность межсетевого экрана, а также проанализированы условия реализации межсетевых экранов в режиме специальной фильтрации.*

Keywords: *special filtering mode, Ethernet, transceiver, virtual connection, model OSI, exponent Hurst, fractal process, queuing system.*

Ключевые слова: *специальный режим фильтрации, Ethernet, приемопередатчик, виртуальное соединение, модели OSI, показатель Хэрста, фрактальный процесс, система массового обслуживания.*

Introduction.

For any business, both small and large, Firewalls something more than a means of network security. At the same time making a decision about their installation may result in unpredictable duration network downtime during the configuration of hardware and software and result in additional costs for labor specialists. If the client wants to receive not only the traditional firewall features, but also guarantee the security of their system traffic or other applications for the realization of such a project would require additional investment. In addition, these requirements greatly complicate the system configuration.

In carrying packet traffic filtering factor limiting the efficiency of Firewalls is the efficiency of packet processing system, operating in accordance with the filtering rules. For evaluate efficiency of the network is usually used parameter bit/s. Under processing in Firewall of packet traffic this parameter is not applicable. For example, a network device that handles 2000 byte packets at a speed of 100 Mbit/s can be handled packet size of 100 bytes at a speed of 12 Mbit/s. If the first case has to handle approximately 10000 packets/s, in the second case the traffic consist of about 40000 packets/s that is four times larger [1]. Therefore, the description of the intensity of the input and output flow, necessary use the integral characteristic efficiency of Firewall, measured as the number of packets per unit time calculated for fixed-size packets.

The structure of the Ethernet packet.

Computer network is sending user data between workstations and servers. All messages sent through the network, broken into fragments of standard length. The structure and sizes of packet is determined by the type and standard protocol network.

Standard 802.3 defines eight header fields:

Preamble field consists of seven bytes of sync data. Each byte contains the same bit sequence - 10101010.

Under Manchester coding, this combination appears in the physical environment periodic wave signal. The preamble is used to give the time and opportunity scheme transceiver to come to the stable synchronism with the receiving clock signal [2].

1. Initial delimiter of frame make up from a single byte with a set of bits 10101011. The appearance of this combination is an indication for the next frame reception.
2. Address the receiver - maybe length a 2 or 6 bytes (MAC-address of the recipient). The first bit of the destination address - it's a sign is the address of the individual or group, if 0 this address points to a specific station, if 1 this group address several of the network stations. Under broadcast address all the bits of the address field set to 1. There is a common use of 6-byte addresses.
3. Source address - 2 or 6-byte field containing the station address of the sender. The first bit - always has a value of 0.
4. Double-byte length field defines the length of the data field in the frame.
5. The data field may contain from 0 to 1500 bytes. But if the length of the field is less than 46 bytes, use the following field - a field of filling to complete the frame to the minimum allowed length.
6. Field filling consists of the number of bytes of such fillers which provides a certain minimum length of the data field (46 bytes). This ensures the correct operation of the mechanism of collision detection. If the length of the data field is sufficient, that field of filling in the frame does not appear.
7. The checksum field - 4 bytes containing the value that is calculated by a certain algorithm. After receiving the frame workstation performs own calculation checksum for this frame, compares the obtained value with the value of the checksum field and thus, detects corrupted or not the received frame.

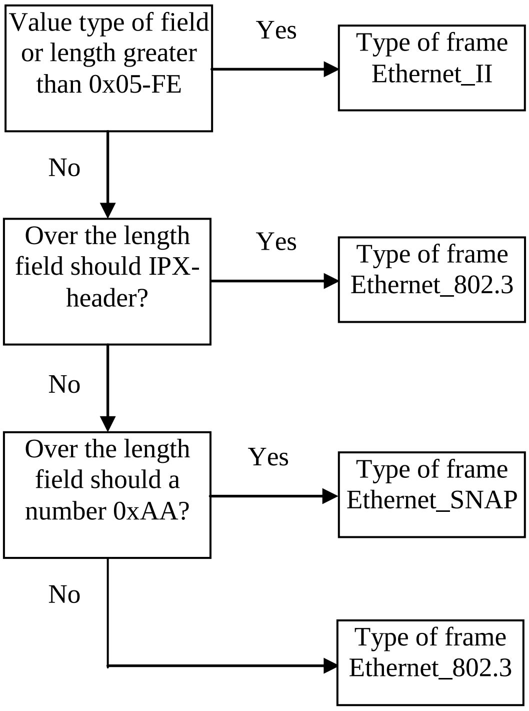
Value type of field or length greater than 0x05-FE
Yes
Type of frame Ethernet_II
No
Over the length field should IPX-header?
Yes
Type of frame Ethernet_802.3
No
Over the length field should a number 0xAA?
Yes
Type of frame Ethernet_SNAP
No
Type of frame Ethernet_802.3

Fig. 1. Algorithm for determining the format of Ethernet frame

The way of calculation of the invariant characteristics for a special filtering mode.

Setting the Firewall in a special filtering mode can be represented as a buffer (see Figure 2). In Figure 2 the following notation: $M -$ the checksum intensity of the processing of all TCP connections (packet/s), $\rho = \lambda / M -$ utilization, $q -$ buffer size (number of packets), $C -$ number of TCP connections, the time existence of which allows us to estimate parameters H : H, H_{in} and $H_{out} -$ the exponent Hurst at the input and output Firewall for allowed TCP connections, $\lambda_i -$ intensity of input flow for the $i -$ th allowed TCP connections, $q_i -$ buffer size allocated for the $i -$ th TCP connection and $m_i -$ intensity of the $i -$ th TCP connection [3-4].

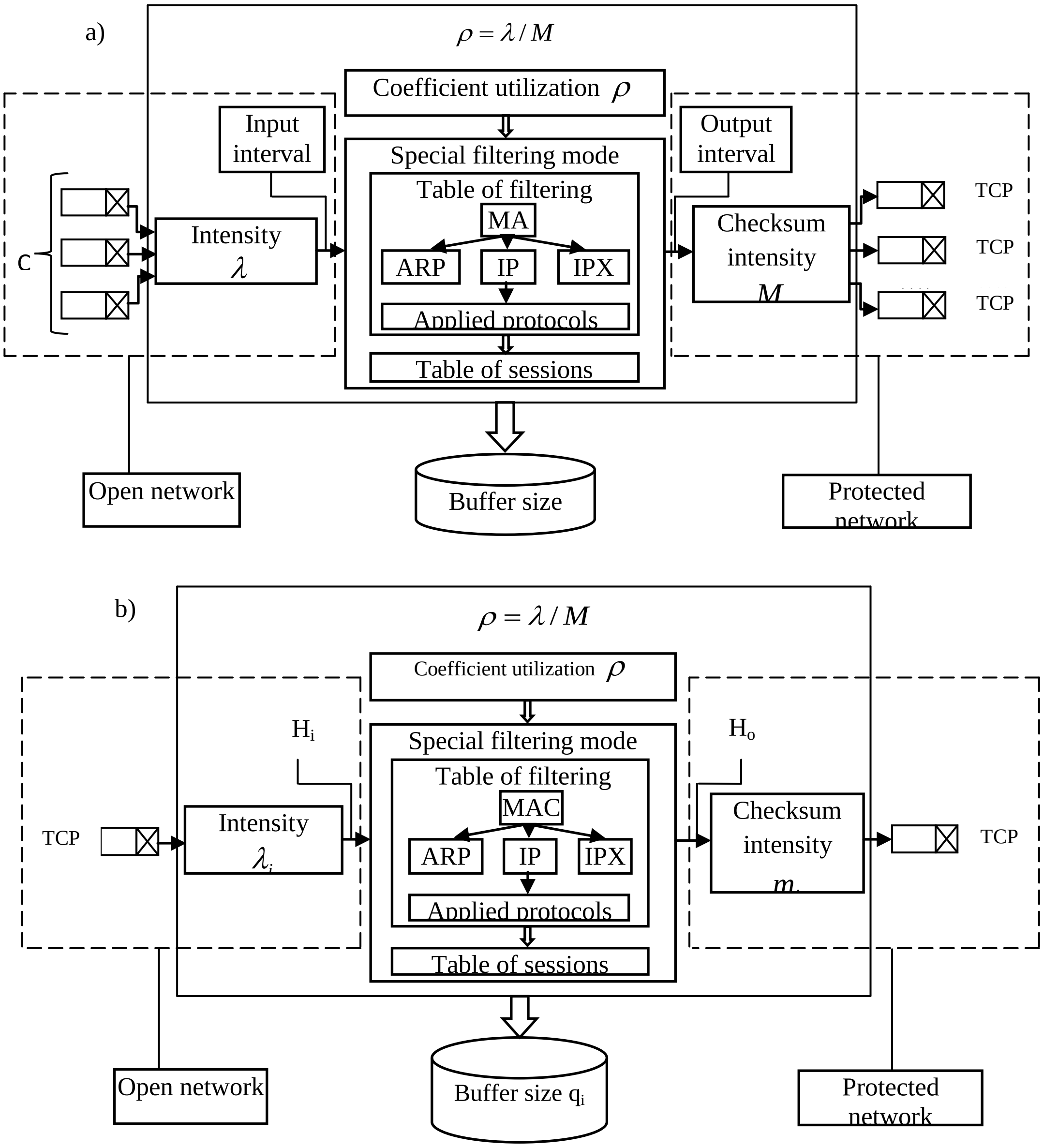

Fig. 2. Architecture Firewall with two physical interfaces: a - general flow, b - a single TCP connection

Parametric conditions special filtering mode.

Under considering data communication in the transport layer of model OSI, the interaction between the source and the receiver data realizes via virtual connection [5]. Although the physical network through which the interaction may consist of a plurality of intermediate nodes: routers, switches, et al. equipment, also and Firewall and have a certain value of the Hurst exponent H (see Figure 3). From the experimental data it is known that the value for global network the value H aggregate flow is in the range 0.6 ÷ 0.8.

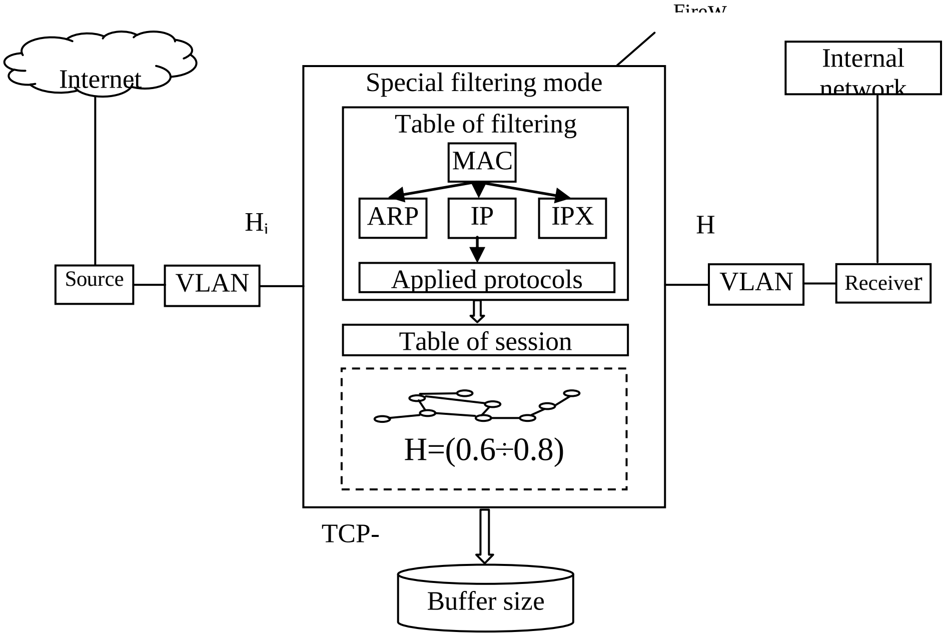

Fig. 3. Displaying model of virtual connection to a physical network

If setting Firewall filtering rules allow packets from the source to the receiver, then this virtual connection will be characterized by some exponent Hurst H. Special filtering mode will provide consistent H in input and output Firewall for this model of virtual connection.

Procedures and conditions for implementation of a special filtering mode

Under processing the input fractal process network device by coefficient utilization p and use the Hurst exponent H there is a level buffer size q which [5] does not happen to be dropping packets and the exponent Hurst H on the input and output Firewall remains unchanged. In queuing system, taking into account the fractal properties of network processes, there are increased demands to the buffer, therefore to calculate its size using the ratio, obtained with the diffusion approximation of the input stream applications. This relationship is as follows:

$$q = \frac{p^{1/2(1-H)}}{(1-p)^{H/(1-H)}}, \qquad (1)$$

where $q -$ buffer size, $p -$ utilization, $H -$ exponent Hurst.

Given that traffic handled by the Firewall, is a set of packets from a variety of transport connection, the above method of calculating the buffer size offers to apply for individual transport connections, allowed to pass through the Firewall. When H is large (based on research findings H is in the range 0.6-0.8) increase in the coefficient p requires a much larger capacity buffer.

Estimation of accuracy for performing the special filtering mode

For the permissible values of the parameters Firewall m_i and q_i need from the expression (1) to obtain depending exponent Hurst H for different values $\lambda_i -$ intensity, $q_i -$ buffer sizes and $m_i -$ performance.

By plotting the exponent Hurst H at different λ_i, q_i and m_i defined ranges of values of m and q for $i -$ th allowed TCP connections [6]. In particular, for the case of network interfaces Firewall 100 Mbit/s, the special filtering mode will be provided at $q_i =$ 50-200 packets and $m_i =$ 4200-9400 packets/sec, which corresponds to the performance 7.8-15.3 Mbit/s.

Figure 6 is presented selection of parameters Firewall with considering the proposed model.

Firewall: $H_{in} = H_{out}$ under $q = 50 - 200$ packets and $m = 14000 - 16000$ packet/s

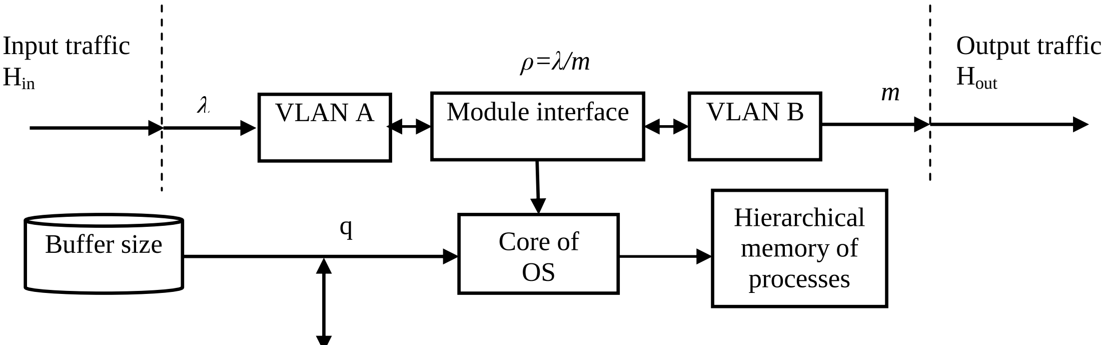

Fig. 6. Firewall with proposed model

Conditions implementation the special filtering mode

The packets are transmitted to the network card and stored in the buffer. When the buffer is filled, the card generates an interrupt and the network card driver copies the data from the buffer card (mbufs) in core memory. Once a packet is transmitted to the mbuf, the execution of all further operations carried out with the packets does not depend on its size, as analyzed only its title. If packet missed necessary, then packet will be sent the network card driver, which will extract it from the mbuf and pass the line. Most of these operations have a relatively high cost per one packet, but a very low cost on the basis of packet size. Therefore, the processing of a large packet is only slightly more expensive than processing a small packet.

Some limitations imposed by hardware tools. For example, machine grade x86-64 not treated with more than 15000 interrupts per second, regardless of the processor speed, which is caused by the limitations architecture. Some network adapter generates one interrupt for each packet. Consequently, the unit will drop packets when their amount exceeds about 15000 packets per second. Other maps, for example, more expensive gigabit have large internal buffer, which allows them to connect multiple packets in a single interrupt. Therefore, the selection of hardware tools may impose some limitations on performance [7].

In the Ethernet environment, the maximum transmission block size that can be transmitted or received adapter is 1538 bytes, which comprises:

- start of frame 8 bytes;
- Ethernet header 14 bytes;
- data up to 1500 bytes;
- checksum 4 bytes;
- packet interval 12 bytes.

The controller is able to send and receive Ethernet frames:

- for 1 Gbit/s - every 12.3 microseconds or about 81,000 frames per second (1,000,000,000 / 1538/8 ~ 81000);
- for 100 Mbit/s - every 123 microseconds or about 8100 frames per second (100,000,000 / 1538/8 ~ 8100).

During normal operation not all network packets have a full size, because their actual number may be much greater importance. Packet processing for such speed requires considerable efficiency, therefore from performance the physical layer performance depends not only the speed of the transmission network, but also the state of the whole system [8]. The work of the network interface can be divided into two stages-this transmit/receive packets and place them in the buffers. Both of these processes are interrelated - before the packet is sent to the network, first it is placed in the buffer of the network card, in the case receive of packet from the network, contrariwise. Driver allocates buffers in physical memory, where the network card stores newly packets. To determine the size of the allocated memory is used, as a rule, two parameters - the number of buffers (one buffer - one packet), which are defined in the configuration of the network card, and the maximum transmission segment (Maximum Transfer Unit MTU). The last parameter is used driver to determine, the amount of memory which necessary pick out under one bufer. If the MTU is not used, it may happen that the allocated buffer is less than that received packet, or is greater than the allocated memory. For example, some network adapters for MTU 1500 allocate 2048 bytes. It is getting, if set the number of buffers in 5000 for incoming packets, the driver will allocate about 10 MB of memory.

Conclusions

In conclusion, might highlight that the exponent Hurst H is an invariant characteristic to the scale of measurement, so his continued input and output of Firewall will be condition a special filtering mode. The developed model of the virtual TCP connection allows the identification of traffic parameters and influence to process of the fractal characteristics. Ranges of values are received under analysis of dependence of the exponent Hurst $H,$ as a function of performance for different values of the buffer size and intensity.

References

1. *Vinod Joseph, Srinivas Mulugu*. Network Convergence: Ethernet Applications and Next Generation Packet Transport Architectures Paperback – November 4, 2013.
2. *Zelenchuk I*. Nastrojka Gigabit Ethernet в ОС GNU / Linux и FreeBSD, 2012.
3. Programmnoe obespechenie, prednaznachennoe dlja rascheta pokazatelja Херста - Selfis. 2007. Access: http://www.cs.ucr.edu.
4. *Gulomov Sh., Abdurakhmanov A. and Nasrullaev N.* Design Method and Monitoring Special Traffic Filtering under Developing «Electronic Government» International Journal of Emerging Technology & Advanced

Engineering (ISSN 2250-2459, ISO 9001:2008 Certified Journal), Volume 5, Issue 1, January, 2015.

5. *Basharin G. L., Bocharov P. P., Kogan Ja. A.* Analiz ocheredej v vychislitel'nyh sistemah. Teorija i metody rascheta. M.: Nauka, 1989.
6. *Karimov M. M., Ganiev A. A., Gulomov Sh. R.* «Models of network processes for describing operation of network protection tools». 4th International conference on application of information and communication technology and statistics in economy and education (ICAICTSEE – 2014) October 24–25th, 2014 University of National and World Economy Sofia, Bulgaria.
7. Adel El-Atawy. An Automated Framework for Validating Firewall Policy Enforcement, POLICY 07: Proceedings of the Eighth IEEE International Workshop on Policies for Distributed Systems and Networks, 151-160, 2007.