Dynamic Firewall Configuration: Security System Architecture and Algebra of the Filtering Rules

Vladimir Zaborovsky[*], Vladimir Mulukha[**], Alexander Silinenko[***], Sergey Kupreenko[****]
St. Petersburg state Polytechnical University
Saint-Petersburg, Russia
vlad@neva.ru[*], vladimir@mail.neva.ru[**], avs@neva.ru[***], ksw@neva.ru[****]

Abstract – **Internet is a global information infrastructure that stores information in the form of distributed digital resources, which have to be protected against unauthorized access. However, the implementations of this protection are far from simple due to dynamic nature of network environment and users activities. We offer a system approach providing a firewall configuration procedure based on new functional model, which includes network monitor, firewall rules generator and the means of rules aggregation. With the help of proposed algebra of filtering rules it is possible to standardize and optimize the dynamic firewall configuration.**

Keywords — dynamic firewall configuration, algebra of filtering rules, access policy, traffic security

I. INTRODUCTION

Internet as a global information infrastructure is used widely for business, education and research. This infrastructure keeps information in the form of distributed digital resources that have to be available for authorized use, while sensitive data should be protected against unauthorized access.

However, the implementations of this protection are far from simple due to the dynamic nature of the network environment state and impossibility of the "security perimeter" organization. Nowadays in virtual networks and clouds, besides securing external network connections, an access control system has to take into account the shared hardware resources and network environment state [1].

The information protection in computer systems has been discussed for almost 50 years. However, the well-known methods of protection of the local data from a remote attacker don't take into account the specifics of modern computer networks such as [2]:

- territorial distribution and concurrency;
- the dual nature of access control procedures that doesn't allow to form a "security perimeter" as a static requirement concerning network services;
- non-locality of network resources and characteristics;
- a semantic gap between security policy description and firewall configuration parameters.

Therefore many well-known security solutions of the past have become increasingly inadequate. That is why currently we need deeper and more detailed understanding of the security processes going on in computer networks. That is why we describe below a system approach to provide a firewall configuration procedure based on new functional model, which includes a network monitor, a firewall rules generator and the means of rules aggregation. The main advantage of the proposed approach is the possibility of constructing an algebra of filtering rules, which allows to aggregate and control the firewall configuration that implements the security requirements. The paper is organized as follows: in Section 2, the architecture of dynamic firewall configuration system and the descriptions of its main components are presented. In Section 3, the usage of the above mentioned algebra is described. Section 4 presents the conclusion and the discussion of the overall results.

II. SECURITY SYSTEM ARCHITECTURE

Internet security is a main issue of modern information infrastructure. This infrastructure stores information in the form of distributed digital resources, which have to be protected against unauthorized access. However, the implementations of this statement are far from simple due to the dynamic nature of the network environment and users activity [3]. Below we describe a new approach to configure the security network appliances, that allows an administrator to overcome the semantic gap between security policy requirements and the ability to configure the firewall filtering rules [1]. The architecture of the proposed system is presented in Fig.1.

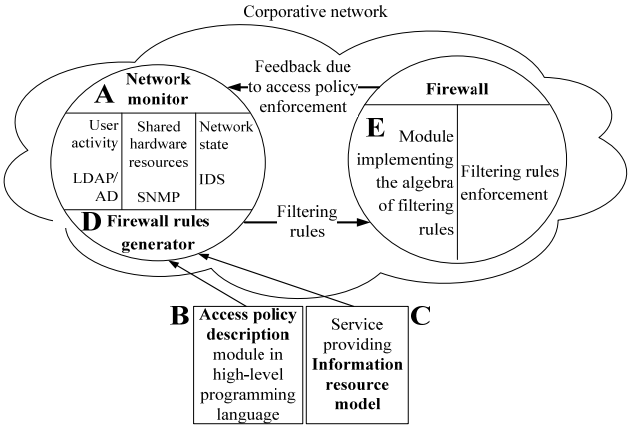

Figure 1. Security system architecture

where:

A. Network monitor

Network monitor controls the whole system. Network environment state consists of three main parts:

- "User activity" is the information about what computer is currently used by which user. This information can be obtained from Microsoft Active Directory (AD) by means of LDAP protocol.
- "Shared hardware resources" is the information about network infrastructure and shared internal resources that can be described by network environment state vector X_k
- "Network state" is the information about external network channel received from Intrusion Detection Systems (IDS).

B. Access policy description module

Filtering rules of a firewall in itself are a formalized expression of an access policy. An access policy may simply specify some restrictions, e.g., "Mr. Black shouldn't work with Youtube" without the refinement of the nature of "Mr. Black" and "work" [4].

There is a common structure of access policy requirements, which uses the notions of subject, action and object. Thus, the informally described requirement "Mr. Black shouldn't work with Youtube" can be formally represented as the combination of the subject "Mr. Black", the action "read", the object "www.youtube.com" and the decision "prohibit". This base can also be augmented by a context, which specifies various additional requirements restricting the cases of rule's application, e.g.: time, previous actions of the subject, attributes' values of the subject or object, etc.

However, access rules, which are based on the notions of subject, action and object are not sufficient alone to implement complex real-world policies. As a result, new approaches have been developed. One of them, Role Based Access Control (RBAC) [5], uses the notion of role. A role replaces a subject in access rules and it's more invariant. Identical roles may be used in multiple information systems while subjects are specific to a particular system. As an example, remember the roles of a system administrator and unprivileged user that are commonly used while configuring various systems. Administrator-subjects (persons) may be being added or removed while an administrator-role and its rules are not changing.

However, every role must be associated with some subjects as only rules with subjects can be finally enforced. During policy specification roles must be created firstly, then access rules must be specified with references to these roles, then the roles must be associated with subjects.

The OrBAC [6] model expands the traditional model of Role Based Access Control. It brings in the new notions of activity, view and abstract context. An activity is to replace an action, i.e., its meaning is analogous to the meaning of a role for a subject. A view is to replace an object. "Entertainment resources" can be an example of view, and "read" or "write" can be examples of an activity. Thus, the notions of role, activity, view and abstract context finally make up an abstract level of an access policy. OrBAC model allows to specify the access rules only on an abstract level using the abstract notions. Those are called the abstract rules. For instance, an abstract rule "user is prohibited to read entertainment resources", where "user" is a role, "read" is an activity, and "entertainment resources" is a view. The rules for subjects, actions and objects are called concrete access rules.

To specify an OrBAC policy, a common language, XACML (eXtensible Access Control Markup Language) was introduced. The language maintains the generality of policy's specification while OrBAC provides additional notions for convenient editing.

C. Firewall rules generator

There is a feature common for all firewalls: they execute an access policy. In common representation the main function of access control device (ACD) is to decide whether a subject should be permitted to perform an action with an object. A common access rule "Mr. Black is prohibited to read www.youtube.com".

As was mentioned above, "Mr. Black" is a subject, "HTTP service on www.youtube.com" is an object, and reading is an action. So the configuration of ACD consists of common access rules that reference the subjects, actions and objects.

Although a firewall as an ACD must be configured with common access rules, each implementation uses its own specific configuration language. The language is often hardware dependent, reflecting the features of firewall's internal architecture, and usually being represented by a set of firewall rules. Each rule has references to host addresses and other network configuration parameters. An example of the verbal description of a firewall rule may go as follows:

> Host with IP address 10.0.0.10 is prohibited to establish TCP connections on HTTP port of host with IP address 208.65.153.238.

The main complexity of this approach is to find out how such elementary firewall rules could be obtained from common access rules.

Each firewall vendor reasonably aims at increasing its sales appeal while offering various tools for convenient editing of firewall rules. However, so far the problem of obtaining firewall rules from common access rules is not resolved in general. Moreover, this problem has not been paid much attention to.

The most obvious issue concerning this problem is that additional information beyond access rules is necessary in order to obtain the firewall rules. This information concerns the configuration of network services and the parameters of network protocols that are used for data exchange – "network configuration". In general, it can be stored among the descriptions of subjects, actions and objects. An example:

> Mr.Black: host with IP-address = 10.0.0.10;
>
> www.youtube.com: HTTP service (port 80) on host with IP-address = 208.65.153.238.

Thus, the final firewall rules can be obtained by addition of the object descriptions to the access rules. It

 ISBN: 978-1-61208-141-0

should be noted that even for small and especially for medium and large enterprises it is necessary to store and manage the network configuration separately from the security policy. The suggested approach allows us to achieve this goal: the security officer can edit the access rules with reference to real objects while the network administrator can edit the parameters of the network objects [7].

It should also be noted that there is no need to specify any fixed rules regarding association of the network parameters with the objects. For instance, HTTP port may be a parameter of an object or it may be a parameter of an action. A criterion is that the most natural representation of access policy must be achieved.

While generating the rules, the parameters of network objects can be automatically retrieved from various data catalogs. DNS is the best example of a world-wide catalog, which stores the network addresses. Microsoft offers the network administrators the powerful means, Active Directory, to store information about users. Integration with the above mentioned technologies greatly simplifies the work of a security officer as he has only to specify the correct name of an object while forming firewall rules.

D. Information resource model

Interaction between subject and object in computer network can be presented as a set of virtual connections. Virtual connections can be classified as technological virtual connections (TVC) or information virtual connections (IVC). (See Fig.2).

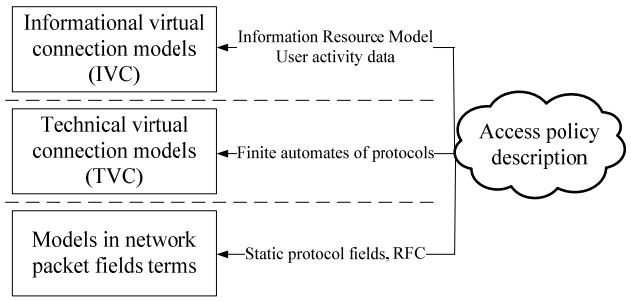

Figure 2. Layers of access control policies.

To implement the policy of access control, the filtering rules are decomposed in the form of TVC and IVC. These filtering rules can be configured for different levels of the data flow description based on the network packet fields at the levels of channel, transport, and application protocols.

At different layers of access control policy model, the filtering rules have to take into account various parameters of network environment and objects. At the packet filter layer, a firewall considers standards static protocol fields described by RFC. At the layer of TVC, firewall enforces the stateful inspection using finite automata describing states of transport layer protocols. On the upper layer of IVC firewall must consider a-priori information about subject and object of network interaction [8].

As was mentioned above, the information about subject can be obtained from catalog services by LDAP protocol, e.g. Microsoft Active Directory.

According to existing approach [9] a resource model can be presented in:

1) logical aspect – an N-dimensional resource space model [10];
2) representation aspect - the definition based on standard high-level description languages like XML or OWL [11];
3) location aspect – the physical storage model of the resource including resource address.

All these approaches describe the network resource as a whole but don't take into account the specific access control task. Any remote network resource can be fully classified when the connection between this resource and local user would be closed. So it is necessary to control all virtual connections in real time while monitoring traffic for security purpose.

In this paper we propose to implement a special service external to the firewall that would collect, store and renew information about remote network objects. It should automatically create information resource model, describing all informational virtual connections that have to be established to receive this resource. This service should periodically renew information about resource to keep it alive.

Firewall should cooperate with this external service to receive information resource model and enforce access policy requirements.

E. Algebra of filtering rules

As was mentioned above, the information security is defined by an access policy that consists of access rules. Each of these rules has a set of attributes; the basic ones among them are identifiers of subject and object and the rights of access from one to another. In TCP/IP-based distributed systems access rules have additional attributes that help to identify flows of packets (sessions) between the client and network application server. Generally these attributes identify the network subjects and objects at different layers of TCP/IP interaction model: MAC-addresses at link layer, IP-addresses at network layer, port numbers at transport layer and some parameters of application protocols.

The access policy in large distributed informational system consists of a huge number of rules that are stored and executed in different access control appliances. The generation of the access policy for such appliances is not very difficult: information must be made available for authorized use, while sensitive data must be protected against unauthorized access. However, its implementation and correct usage is a complex process that is error-prone. Therefore the actual problem of rule generation is representation, analysis and optimization of access policy for large distributed network systems with lots of firewall filtering rules. Below we propose an approach to description, testing and verification of access policy by the

 ISBN: 978-1-61208-141-0

means of specific algebra with carrier being the set of firewall filtering rules.

According to proposed approach we define a ring as algebraic structure over set of filtering rules or R [12]. This ring consists of the following operations over the elements of the set R:

1. Commutativity of addition: $\forall a,b \in R \;\; a + b = b + a$.
2. Associativity of addition: $\forall a,b,c \in R \;\; a + (b + c) = (a + b) + c$.
3. Zero element of addition: $\forall a \in R \; \exists 0 \in R: \;\; a + 0 = 0 + a = a$.
4. Inverse element of addition: $\forall a \in R \; \exists b \in R: \;\; a + b = b + a = 0$.
5. Associativity of multiplication: $\forall a,b,c \in R \;\; a \times (b \times c) = (a \times b) \times c$.
6. Distributivity: $\forall a,b,c \in R \begin{cases} a \times (b + c) = a \times b + a \times c \\ (b + c) \times a = b \times a + c \times a. \end{cases}$
7. Identity element: $\forall a \in R \; \exists 1 \in R: \;\; a \times 1 = 1 \times a = a$.
8. Commutativity of multiplication: $\forall a,b \in R \;\; a \times b = b \times a$.

Let's define the algebra of filtering rules R = <R, Σ>, where R – the set of filtering rules, Σ – the set of possible operations over the elements of R. The set of filtering rules $R = \{r_j, j=\overline{1,|R|}\}$ – the carrier set of algebra R. Every rule $r_j = \{X_1,\ldots,X_N, A_j, B_1,\ldots B_M\}_j$ consists of a vector X_j of parameters, a binary variable A_j and a vector B_j of attributes. $A_i \in \{0,1\}$ is a mandatory attribute that defines the action of access control system over packets; A_j=0 means that packets must be dropped (access denied), A_j=1 means that packets must be passed to receiver (access allowed); $B_{ij} \in DB_j$ is a vector of attribute sets lengths to M (M can be 0). An example of elements of X_j: X_{j1} will be the set of client IP-addresses, and X_{j2} the set of server TCP-ports. The rule attributes B_j define the behavior of access control system that must be applied to corresponding flow of packets (session). The sets of possible values of parameter and attribute vectors are $DX_1,\ldots,DX_N$ and $DB_1,\ldots,DB_M$ in accordance with semantics of every parameter and attribute. For carrier set R the following expression is right (here "×" is the symbol of Cartesian product):

$$R \subset DX_1 \times DX_2 \times \ldots \times DX_N \times DA \times DB_1 \times \ldots \times DB_M$$

The set $\Sigma=\{\varphi_1,\varphi_2\}$ defines the operations that are possible over filtering rules , where φ_1 is the operation of addition, φ_2 is the operation of multiplication.

The operation of addition for filtering rules is defined by the following expressions [12]:

$$r_3 = r_1 + r_2 = \{X_{11}, X_{12},\ldots X_{1N}, A_1, B_{11},\ldots, B_{1M}\} + \\ + \{X_{21}, X_{22},\ldots X_{2N}, A_2, B_{21},\ldots, B_{2M}\}$$

$$r_3 = \begin{cases} \{X_{11} \cup X_{21},\ldots X_{1N} \cup X_{2N}, A_1 \vee A_2, B_{11} \cup \\ \cup B_{21},\ldots, B_{1M} \cup B_{2M}\}, \text{if } A_1 = A_2; \\ \\ \{X_{11} \Delta X_{21},\ldots X_{1N} \Delta X_{2N}, A_1 \wedge \\ \wedge A_2, B_{11} \Delta B_{21},\ldots, B_{1M} \Delta B_{2M}\}, \text{if } A_1 \neq A_2, \end{cases}$$

where A_i is the the attribute "the action of rule", $\cup$ is the union of sets, Δ is the symmetrical difference of sets, $\vee$ and $\wedge$ are the logical disjunction and conjunction respectively. In other words the sum of two filtering rules is

4) union of sets of the same name parameters and attributes if the attribute "the action of rule" is equivalent in both rules;
5) symmetrical difference of sets of the same name parameters and attributes if the attribute "the action of rule" is different in summand rules.

The operation of multiplication for filtering rules is defined by following expressions:

$$r_3 = r_1 \times r_2 = \{X_{11}, X_{12},\ldots X_{1N}, A_1, B_{11},\ldots, B_{1M}\} \times \\ \times \{X_{21}, X_{22},\ldots X_{2N}, A_2, B_{21},\ldots, B_{2M}\}$$

$$r_3 = \{X_{11} \cap X_{21}, X_{12} \cap X_{22},\ldots X_{1N} \cap X_{2N}, \\ A_1 \wedge A_2, B_{11} \cap B_{21},\ldots, B_{1M} \cap B_{2M}\},$$

where $\cap$ – intersection of sets. In other words the product of two filtering rules is intersection of sets of the same name parameters and attributes; attribute "the action of rule" for result rule is a conjunction of corresponding attributes of initial rules.

Zero 0_r, identity 1_r and inverse –r elements of R are specifies by following expressions:

$$0_r = \{\varnothing, \varnothing,\ldots \varnothing, A, \varnothing,\ldots, \varnothing\}, \; A = 0$$

$$1_r = \{DX_1, DX_2,\ldots, DX_N, A, DB_1,\ldots, DB_M\}, \; A = 1$$

$$-r = \{X_1, X_2,\ldots, X_N, \overline{A}, B_1,\ldots, B_M\},$$

where $\overline{A}$ – logical inversion of A

The described algebra is distributive commutative ring with identity element that means execution of corresponding axioms.

III. Firewall Configuration Using Proposed Algebra

Let's specify the element of set R as r = {X_1, X_2, A} where X_1 – subset of source IP-addresses, DX_1 = [0.0.0.0, 255.255.255.255]; X_2 – subset of destination IP-addresses, DX_2 = [0.0.0.0, 255.255.255.255]; A – attribute "the action of rule", DA = {0,1}, 0 denies access, 1 allows access; let M=0, so there would be no B_{ij} attributes. It is necessary to define the full and consistent access policy that allows establishing of sessions from Internal network (see schema on Fig.3, a) to External subnetworks 0.0.0.0 – 9.255.255.255, 20.0.0.0 – 49.255.255.255 and from External subnetworks 40.0.0.0 – 49.255.255.255 to the whole Internal network.

For this task a convenient method of representation of access policy is 2-dimensional space x_1x_2. Every point of this space is specified by the coordinates (x_1, x_2). The set of points (x_1, x_2) is specified by Cartesian product of sets DX_1 and DX_2 (see on Fig.3, b).

 ISBN: 978-1-61208-141-0

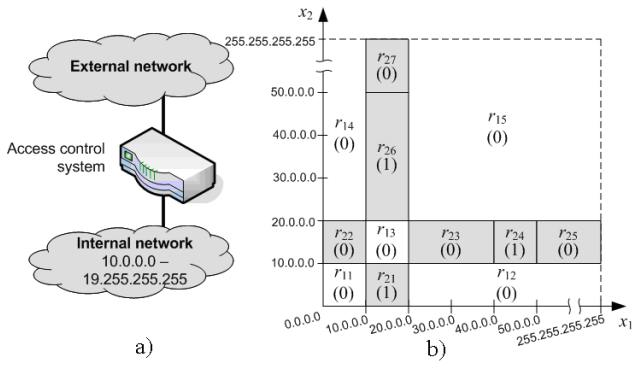

Figure 3. Access control system based on firewall (a) and access policy as a space of parameters (b)

Definition 1. The access policy is full if filtering rules specify the whole of space of parameters:

$$\forall x_1 \in DX_1, x_2 \in DX_2 ..., x_N \in DX_N \ (x_1, x_2, ..., x_N) \in$$
$$\in \bigcup_{i=1}^{|R|} (X_{i1}, X_{i2}, ..., X_{iN})$$

Definition 2. The access policy is consistent if any point of space of parameters belongs only to one filtering rule:

$$\bigcap_{i=1}^{|R|} (X_{i1}, X_{i2}, ..., X_{iN}) = \varnothing .$$

Obviously that for schema on Fig. 3 there are some forbidden areas that are incorrect from the point of view of IP-network functionality. The following rules describe such areas (in Fig. 9,b these areas are colored in white):

r_{11} = {0.0.0.0 – 9.255.255.255; 0.0.0.0 – 9.255.255.255; 0};
r_{12} = {20.0.0.0 – 255.255.255.255; 0.0.0.0 – 9.255.255.255; 0};
r_{13} = {10.0.0.0 – 19.255.255.255; 10.0.0.0 – 19.255.255.255; 0};
r_{14} = {0.0.0.0 – 9.255.255.255; 20.0.0.0 – 255.255.255.255; 0};
r_{15} = {20.0.0.0 – 255.255.255.255; 20.0.0.0 – 255.255.255.255; 0}.

Let us optimize this set of rules by applying the algebra's addition operation to rules r_{11} and r_{14}, r_{12} and r_{15}:

$r_{17} = r_{11} + r_{14}$ = {0.0.0.0 – 9.255.255.255; 0.0.0.0 – 9.255.255.255, 20.0.0.0 – 255.255.255.255; 0};
$r_{18} = r_{12} + r_{15}$ = {20.0.0.0 – 255.255.255.255; 0.0.0.0 – 9.255.255.255, 20.0.0.0 – 255.255.255.255; 0}.

For other areas (colored gray in Fig. 3,b) it is necessary to specify the filtering rules according to the task conditions:

r_{21} = {10.0.0.0 – 19.255.255.255; 0.0.0.0 – 9.255.255.255; 1};
r_{22} = {0.0.0.0 – 9.255.255.255; 10.0.0.0 – 19.255.255.255; 0};
r_{23} = {20.0.0.0 – 39.255.255.255; 10.0.0.0 – 19.255.255.255; 0};
r_{24} = {40.0.0.0 – 49.255.255.255; 10.0.0.0 – 19.255.255.255; 1};
r_{25} = {50.0.0.0 – 255.255.255.255; 10.0.0.0 – 19.255.255.255; 0};
r_{26} = {10.0.0.0 – 19.255.255.255; 20.0.0.0 – 49.255.255.255; 1};
r_{27} = {10.0.0.0 – 19.255.255.255; 50.0.0.0 – 255.255.255.255; 0}.

These rules may be optimized also by applying of algebra's addition operation:

$r_{28} = r_{21} + r_{26}$ = {10.0.0.0 – 19.255.255.255; 0.0.0.0 – 9.255.255.255, 20.0.0.0 – 49.255.255.255; 1};
$r_{29} = r_{22} + r_{23}$ = {0.0.0.0 – 9.255.255.255, 20.0.0.0 – 39.255.255.255; 10.0.0.0 – 19.255.255.255; 0}.

As a result the access policy describes by following filtering rule set:

$$R = \{r_{13}, r_{17}, r_{18}, r_{24}, r_{25}, r_{27}, r_{28}, r_{29}\}.$$

The dimension of R is the main attribute that describes firewall performance characteristics. Usage of the algebraic operations of addition and multiplication allows us to reduce dimensionality of R and thus to increase the firewall performance while fulfilling requirements of the specific security policy [12]. However the correctness of each rule depends on an environment condition, which can vary in real time. Therefore static description of access policy by means of proposed algebra is not enough and according to the telematics approach it is necessary to consider an environment condition with statistical parameters. Development of randomized model of the network environment considering these requirements, allows us to increase accuracy of the description of an access policy by means of filtering rules.

IV. CONCLUSION.

1. Each firewall is required to work in compliance with a security policy, user activities and network configuration. Policy requirements cannot be considered separately from methodology of proper firewall configuration and specified security characteristics. Based on OrBAC model it is possible to translate high-level abstract security requirements to low-level firewall configuration.

2. Firewall configuration can be largely automated based on specifying high-level access rules and parameters of corporate DNS, AD/LDAP, SNMP and IDS services. Proposed system architecture can be easily implemented due to consideration of role-based information access models and characteristics of specific firewalls.

3. Proposed algebra of filtering rules is a new mathematical description of access policy and a formal tool for firewall configuration. The system approach provides possibility to prove fullness and consistency of an access policy. The proposed algebra is the base of optimization of the set of filtering rules and of the design of dynamic firewall configuration.

REFERENCES

[1] V. Mulukha. Access Control in Computer Networks Based on Classification and Priority Queuing of the Packet Traffic, PhD. Thesis 05.13.19, SPbSPU, Russia, 2010

[2] V. Zaborovsky and V. Mulukha. Access Control in a Form of Active Queuing Management in Congested Network Environment // Proceedings of the Tenth International Conference on Networks, ICN 2011 pp.12-17.

[3] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. 2010. A view of cloud computing. Commun. ACM 53, 4 (April 2010), pp.50-58.

[4] A. Titov and V. Zaborovsky. Firewall Configuration Based on Specifications of Access Policy and Network Environment // Proceedings of the 2010 International Conference on Security & Management. July 12-15, 2010.

[5] D.F. Ferraiolo and D.R. Kuhn. Role-Based Access Control. 15th National Computer Security Conference. (October 1992), pp. 554–563.

 ISBN: 978-1-61208-141-0

(http://csrc.nist.gov/groups/SNS/rbac/documents/ferraiolo-kuhn-92.pdf)

[6] Organisation-based access control (OrBAC.org). Available: http://orbac.org/index.php?page=orbac&lang=en

[7] V. Zaborovsky and A. Titov. Specialized Solutions for Improvement of Firewall Performance and Conformity to Security Policy // Proceedings of the 2009 International Conference on Security & Management. v. 2. pp. 603-608. July 13-16, 2009.

[8] V. Zaborovsky, A. Lukashin, and S. Kupreenko Multicore platform for high performance firewalls. High performance systems // Materials of VII International conference – Taganrog, Russia.

[9] H. Zhuge, The Web Resource Space Model, Berlin, Germany: Springer-Verlag, 2007

[10] H. Zhuge, "Resource Space Grid: Model, Method and Platform," Concurrency and Computation: Practice and Experience, vol. 16, no. 14, pp. 1385-1413, 2004

[11] D. Martin, M. Burstein, J. Hobbs, O. Lassila. et al. (November 2004) "OWL-S: Semantic Markup for Web Services," [Online]. Available: http://www.w3.org/Submission/OWL-S/.

[12] A. Silinenko. Access control in IP networks based on virtual connection state models: PhD. Thesis 05.13.19: / SPbSTU, Russia, 2010.

 ISBN: 978-1-61208-141-0