КОМПЬЮТЕРНЫЕ НАУКИ

УДК 681.518

МЕТОД ФОРМИРОВАНИЯ ДЕЙСТВУЮЩЕЙ ПОЛИТИКИ ДОСТУПА К РЕСУРСАМ КОМПЬЮТЕРНОЙ СЕТИ

САЕНКО В.И., ГОЛУБЕВ А.С.

Рассматривается подход к решению проблемы оперативного управления – контроля использования разделяемых ресурсов в компьютерных сетях. Разрешающее либо запрещающее воздействие определяется действующим правилом и формируется сервером контроля доступа на основе анализа множества прав. Действующая политика является множеством, состоящим из всех действующих прав для данной сети.

1. Проблема контроля доступа к ресурсам в компьютерной сети

В корпоративных компьютерных сетях, насчитывающих большое число компьютеров, всегда существует проблема распределения прав доступа к ресурсам и оперативного контроля их использования. Сложность сети обуславливает наличие большого количества требований доступа пользователей и их групп к множеству ресурсов. В настоящее время в корпоративных сетях формируются специальные наборы правил, позволяющие удовлетворить возникающие требования. Правила объединяются в политики. Средствам администрирования требуется при поступлении запроса от пользователя оперативно выработать решение о запрете либо доступе к соответствующему ресурсу. При этом следует учесть существующее распределение доступа и существующие наборы правил (политик). Динамически необходимо определить действующие правила (политику).

Предлагаемая статья является продолжением статьи [4]. В ней был рассмотрен метод формирования и описания политики доступа к ресурсам.

2. Анализ известных результатов исследований в области контроля доступа к ресурсам

На сегодняшний день одним из самых перспективных направлений решения проблем менеджмента является разработка метода администрирования на основе концепции политик [1].

Наиболее эффективным считается подход на основе объектно-ориентированного представления элементов сети – CIM – Common Information Model (Общая информационная модель) [2, 3]. Данный стандарт описывает свойства и методы информационных объектов, а также регламентирует взаимосвязи между ними. Вводятся правила именования. Стандарт описывает политики как информационный объект, специфицирует принципы функционирования (условие-действие). Однако конкретная схема принятия решений на основе набора политик в информационной модели отсутствует.

В [4] предложен метод формирования и описания политик с разделением на политики ресурсов и пользователей, использованием стратегий. Однако в работе отсутствует описание процесса анализа политик при принятии решения средствами контроля доступа о разрешении либо запрете использования разделяемого ресурса.

В [5] рассматривалось применение политик для упрощения настройки брандмауэра. Были освещены возможные случаи противоречий, возникающих в процессе редактирования, представлены способы выявления и разрешения конфликтов. Проблема противоречий и сложности анализа политик решалась объединением (изменением) политик на этапе их создания и построения древовидной модели политик. В данной модели корневой вершиной является протокол, а листьями – разрешения, либо запрет политики. Проблема оперативного управления запросами решалась путем нахождения соответствующего запросу маршрута в дереве от корня к листу. Основные операции проводились с IP адресами отправителя и получателя, сами же пользователи не учитывались.

Цель исследования состоит в разработке метода оперативного формирования правил доступа к ресурсам по запросам пользователей в условиях наличия множества требований по ограничению доступа.

3. Постановка задачи

Пусть есть компьютерная сеть. В сети присутствуют процессы, порождающие информационные потоки в результате обмена информацией между приложениями пользователей и ресурсов Интернет. Приложения, формирующие потоки, запрашивают ресурсы у сервера Proxy, образуя соединения. Процессы обладают определенными правами, соответствующими правам пользователей.

Требуется сформировать метод в соответствии с семантикой задания правил [4], по которым Proxy сервер смог бы осуществлять контроль использования пользователями ресурсов, путем разрешения либо запрета запроса на соединение.

4. Описание объекта исследования

Пусть имеется некоторая корпоративная компьютерная сеть *Net* с централизованным администрированием. Пусть имеется общий ресурс *Res*, например, логический канал доступа к Интернет. Доступ осуществляется через сервер контроля доступа – Proxy сервер.

В сети активны некоторое количество M пользователей {*users*} и групп G={*groups*}, в которые пользователи могут быть объединены.

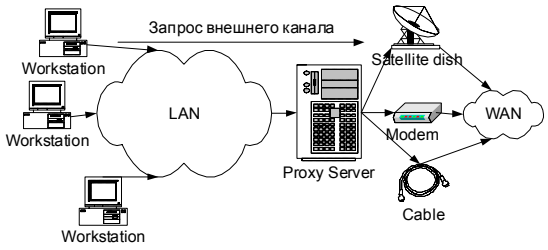

Схема доступа к ресурсам

Пользователи через программные приложения получают доступ к каналу Интернет. Будем далее полагать, что пользователь представлен в сети определенным набором процессов proc (i, uid), где uid - идентификатор пользователя. Считаем, что права acc(uid), которыми обладает процесс в сети, определены для породившего его пользователя.

Факт доступа к ресурсам пользователя будем описывать логическим объектом "Соединение", предложенным в [4].

Соединение – это логическая функция, означающая некоторую связь хостов для обмена информацией, заданную уникальным идентификатором соединения cid, которому соответствует трафик (f_j) (поток данных), характеризуемая граничным шлюзом (proxy_id), адресом (именем) требуемого ресурса (addr_rec), адресом (именем) отправителя (addr_snd) и видом сервиса (serv). Соединение -

$$\mathrm{Conn_j(cid, proc(i,uid), proxy\_id, addr\_rec,}$$
$$\mathrm{addr\_snd, serv).} \qquad (1)$$

Задачей сервера контроля доступа является принятие запросов на соединение, анализ этих запросов, политик доступа, и, в конечном итоге, формирование разрешения либо запрета на соединение.

Примем концепцию [4], согласно которой в сети заданы стратегии формирования политик: стратегия для ресурса St_Resource и стратегия для пользователей St_Users**.** Стратегия для ресурса описывает распределение прав к конкретному ресурсу относительно множества пользователей. Стратегия для пользователей определяет доступ к множеству ресурсов относительно пользователя.

Согласно стратегиям формируются политики доступа для пользователей и ресурсов. Будем использовать комбинированный метод управления доступом к ресурсам, основанный на определении политик как прав доступа относительно групп и пользователей, и отдельно прав доступа к ресурсам (рисунок).

Согласно [4] в сети будем использовать стратегии распределения ресурсов. Примем за основную *Стратегию D.* Пользователи получают доступ к ресурсам без ограничений на полосу пропускной способности, при разных групповых приоритетах и разных личных приоритетах, по принципу обычной очереди с полным обслуживанием за время сеанса.

Оперативное управление доступом осуществляется на основании списков доступа и маркеров доступа в смысле [4].

Маркер доступа – это множество элементов, соответствующих группам, в которые входит пользователь прямо или косвенно, элемент личного приоритета пользователя и его идентификатор.

Маркер доступа

$$P = (\{u_i, r_i\}, \{g_1, r_1\}, \{g_2, r_2\} \ldots \{g_l, r_l\}),$$

если $u_i \subset g_k, k = 1..l, u_i \in M, g_k \in G$.

Для возможности реализации вычислительных процедур в сети маркер доступа будем представлять через идентификаторы групп:

$$P_u = \{\{uid_u, r_u\}, \{gid_u^1, r_u^1\}, \{gid_u^2, r_u^2\}, .., \{gid_u^h, r_u^h\}\}, \quad (2)$$

где

$$h = |G'_u|, u \in M, uid_u \leftrightarrow u, gid_u^i \leftrightarrow g, u \subset g, \; i = 1..h, G'_u$$

– набор групп, в которые входит пользователь u, uid_u – идентификатор пользователя u, gid_u^i – идентификатор группы, в которую входит пользователь u; r_u^i – приоритет для gid_u^i ; r_u – приоритет для пользователя u.

Список доступа – множество элементов, определяющее права для любого соединения в компьютерной сети. Каждый элемент списка будет разрешать либо запрещать генерацию трафика некоторому пользователю или группе для некоторого ресурса. Список доступа имеет такую структуру:

L={t,E}, где t – запись, регламентирующая доступ по умолчанию (для всех):

$$t = \{right'\}, right' \in \{allow, deny\},$$

E – запись определяет правило – разрешение либо запрет использования ресурса для некоторого пользователя, группы. Доступ по умолчанию регламентируется самой первой записью.

Для повышения эффективности управления сетью будем использовать приоритет для групп и пользователей.

Приоритет – Pr числовая характеристика группы либо пользователя. Возможно создавать условия, когда группа имеет более высокий приоритет, как условия, когда пользователь имеет более высокий приоритет.

Пусть приоритеты могут принимать значения Pr={0,1,2,3}, где 0 – самый низкий (присваивается в случае, если приоритет не определен), 3 – самый высокий приоритет. При равных приоритетах пользователя и группы запрет имеет больший приоритет, чем разрешение.

5. Примеры использования приоритетов

Пример 1. Пусть пользователь входит в группу G, которой запрещен доступ к ресурсу Res_j. Но для пользователя делается исключение и в личной политике устанавливается право доступа к ресурсу (приоритет – 1). Тогда пользователь все равно получит доступ к ресурсу.

Пример 2. Пусть пользователь входит в группу G, которой запрещен доступ к ресурсу Res_j. И для всей группы устанавливается высокий уровень запрета доступа (флаг приоритета – 2). Но для пользователя делается исключение и в личной политике устанавливается право доступа к ресурсу (но приоритет – 1). Тогда пользователь все равно не получит доступ к ресурсу, так как приоритет группы выше.

Такой метод формирования политик позволяет создавать алгоритмы управления доступом в реальном режиме времени.

Пример 3. Пусть существует некоторое множество соединений. Пусть возникают условия, связанные с требованиями о срочном снижении трафика. Тогда для целой группы пользователей устанавливается более высокий приоритет и вступает в силу требование о запрете доступа к ресурсу.

6. Описание семантики понятий метода определения действующей политики

Будем различать следующие семантические понятия:

1. Ресурсом (*resource*) будем называть любой элемент сети, который может быть разделен между пользователями.

2. Объектом доступа (AO) - является пользователь (*user*) либо группа пользователей (*group*).

3. Запрос и *соединение*. Соединение $Conn_j$ является логической функцией, означающей связь хостов для передачи информации:

$Conn_j$(cid, proc(i,uid), proxy_id, addr_rec, addr_snd, serv).

При $Conn_j$=true имеем логическую связь хостов. При $Conn_j$=false имеем отклоненную попытку пользователя соединиться с некоторым хостом. Запрос на соединение $Reqv_j$ – это информационный объект, элемент сети, используемый для установки соединения (нахождения значения функции $Conn_j$):

$Reqv_j$=(cid, proc(i,uid), proxy_id, addr_rec, addr_snd, serv).

4. Политика доступа P_i – это набор правил: P_i={R}, где R – множество правил.

5. Правило доступа R_j – логическое выражение, формирующее действие:

$$\mathrm{Rule}_j = \begin{cases} \text{if } (\mathrm{cond}_j = \text{true}) \text{ then run}(a_1); \\ \text{if } (\mathrm{cond}_j = \text{false}) \text{ then run}(a_2), \end{cases}$$

где $cond_j$ – логическое выражение – условие правила, a_1 – действие, которое выполняется при $\mathrm{cond}_j = \text{true}$, a_2 – действие, которое выполняется при $\mathrm{cond}_j = \text{false}$, run – функция запуска команды действия на выполнение.

6. Действующее правило доступа – логическое выражение, определяющее действие – отклонение либо принятие запроса:

$$\overline{\mathrm{Rule}_i} = \begin{cases} \text{if } (\mathrm{Conn}_i = \text{true}) \text{ then run(accept)}; \\ \text{if } (\mathrm{Conn}_i = \text{false}) \text{ then run(reject)}. \end{cases}$$

В данной задаче $Conn_i$ – соединение, как логическая функция, действие accept – принятие запроса (a_1), reject – отклонение запроса (a_2). $Conn_i$ вычисляется на основе прав доступа:

7. Право доступа E_i – это информационный объект, регламентирующий отношение двух элементов - ресурса и объекта доступа.

$\mathrm{E_i} = (\mathrm{AO_j}, \mathrm{right_i}, \mathrm{Resource_k})$, где AO_j – некоторый объект доступа, $\mathrm{right_i} = \{\text{allow}, \text{deny}\}$ – разрешение либо запрет доступа, $Resource_k$ – ресурс. В данной задаче, в соответствии с [4], полагаем, что:

$$\mathrm{E_i} = (\mathrm{sid_j}, \mathrm{right_i}, \mathrm{Reqv_k}),$$

где $\mathrm{sid_j} \in \{\text{uid}, \text{gid}\}$ – идентификатор пользователя либо группы, $\mathrm{right_i} \in \{\text{allow}, \text{deny}\}$.

Различают право пользователя и право ресурса.

8. Право доступа к ресурсу – это право, в котором объект доступа не определен AO_j=*, $\mathrm{E_i^r} = (*, \mathrm{right_i}, \mathrm{Resource_k})$. $(\mathrm{AO_j} = *) \Leftrightarrow (\forall \mathrm{AO_j})$ – для всех объектов доступа.

9. Право доступа пользователя – это право, в котором определен ресурс и объект доступа.

10. Право E_i *конкретизирует* E_j, если $\mathrm{Resource_k} \subseteq \mathrm{Resource_l}$, где $\mathrm{Resource_k} \in \mathrm{E_i}$ и $\mathrm{Resource_l} \in \mathrm{E_j}$.

7. Анализ использования предложенной семантики

Каждый пользователь обладает некоторыми привилегиями и может запрашивать множество соединений с внешними (за пределами сети предприятия) ресурсами.

При запросе пользователя $Reqv_i$ серверу контроля доступа необходимо проверить наличие прав, разрешающих работу с конкретным ресурсом. Это происходит посредством анализа множества прав. Если пользователю позволено запрашивать такое соединение, то необходимо выделить некоторую часть ресурса канала. При невозможности такого выделения вследствие загруженности запрос отклоняется.

Будем полагать, что в сети существует множество трафиков, характеризуемых соединениями $\{\mathrm{f_j}, \mathrm{Conn_j}\}$. Существует также множество запросов $\{\mathrm{Reqv_i}\}$, желающих получить соответствующие соединения. По факту только часть из этих запросов получит разрешение на установление соединения. Принятие решений осуществляется в соответствии с заранее установленными требованиями и правами.

8. Метод определения действующего правила

Предлагается метод формирования действующего правила доступа к ресурсам путем оценивания прав пользователя и групп, в которые он входит. Метод учитывает конкретизацию политик ресурса политикой пользователя, использует приоритеты пользователей и групп.

Для определения действующего правила необходимо придерживаться следующей последовательности действий.

1. При получении запроса на соединение $Reqv_i$ сервер контроля доступа распознает пользователя u по его идентификатору uid, получает маркер доступа пользователя P_u, сделавшего запрос.

2. Proxy сервер выбирает пользовательские права доступа E_i из списка доступа L, формируя оперативный список доступа для конкретного запроса $L^1=\{E^1\}=\{E^1_1, E^1_2, ..., E^1_n\}$. Для E^1_i – верхний индекс означает принадлежность к L^1, нижний индекс является однозначным идентификатором элемента внутри множества L^1.

Выборка осуществляется $\forall E_i \in L$ по следующему правилу:

$$R_u = ((sid' \neq *) \,\&\&((sid_1 = sid') \,\|\, (sid_2 = sid') \,\|\, ... \,\|\, (sid_n = sid')) \,\&\&\, (proxy\_id = proxy\_id') \,\&\&\, (addr\_snd \cap addr\_snd' \neq \emptyset) \,\&\&\, (addr\_rec \cap addr\_rec' \neq \emptyset) \,\&\&\, (serv \cap serv') \neq \emptyset) = true, \quad (3)$$

где, полагая, что

$$x' \in \{sid', proxy\_id', addr\_snd', addr\_rec', serv'\},$$

имеем $x' \in Reqv_i$ и, полагая, что

$$x \in \{sid_i, proxy\_id, addr\_snd, addr\_rec, serv\},$$

имеем $x \in E_i$.

3. Формируем новый список L^2 из L^1. $L^2=\{E^2_s\}, E^2_s=\{E^2_{s1}, E^2_{s2}, ..., E^2_{sn}\}$. Множество L^2 состоит из прав E^2_{si} пользователя и групп, в которые он входит согласно P_u, $\forall si \Leftrightarrow sid_i \in P_u, n=|P_u|$. $E^2_{si}=\{e^1_{si}, e^2_{si}, ..., e^k_{si}\}$ – каждое право для конкретного пользователя или группы также представляет собой множество. $e^j_{si}=(sid_{si}, right^j_{si}, Conn^j_{si})=E_i \in L$ – право объекта доступа, $j=1..k$, $k=|E^2_{si}|$. E^2_{si} – множество прав пользователя.

4. Формируем $L^3=\{E^3_{s1}, E^3_{s2}, ..., E^3_{sn}\}$ из L^2, дополняя пустые права правом по умолчанию.

Если $E^2_{si}=\emptyset, E^2_{si} \in L^2$, то $E^3_{si}=\{t\}, E^3_{si} \in L^3$.

Если $E^2_{si} \neq \emptyset, E^2_{si} \in L^2$, то $E^2_{si} \to E^3_{si}, E^3_{si} \in L^3$.

5. Формируем множество прав ресурсов $E^r=\{E^r_1, E^r_2, E^r_n\}$ из L по условию (sid=*) для всех прав $\forall E_i \in L$.

6. Формируем L^4, для этого дополняем L^3 правами ресурсов из E^r. E^r_j добавляем в множество E^4_{si}, если хотя бы для одного из элементов $e^j_{si} \in E^3_{si}$ выполняется правило:

$$R_r = ((proxy\_id = proxy\_id') \,\&\&\, (addr\_snd \subseteq addr\_snd') \,\&\&\, (addr\_rec \subseteq addr\_rec') \,\&\&\, (serv \subseteq serv')) = true, \quad (4)$$

где, полагая, что

$$x' \in \{sid', proxy\_id', addr\_snd', addr\_rec', serv'\},$$

имеем $x' \in E^r_j$ и, полагая, что

$$x \in \{sid_i, proxy\_id, addr\_snd, addr\_rec, serv\},$$

имеем $x \in e^j_{si}$.

Выражение (4) принимает значение истина тогда и только тогда, когда право пользователя $e^j_{si}=E_i$ является уточнением права для ресурса E^r.

7. Каждый $E^4_{si} \in L^4$ преобразуем в $E^5_{si}=(sid_{si}, right_{si}) \in L^5$, $right_{si}=\{allow, deny\}$, $sid_{si} \in P_u$ (или $sid_{si}=*$ для прав ресурсов), т.е. определяем результирующее правило (5) для каждого объекта доступа. При принятии однозначного соответствия $allow \Leftrightarrow true, deny \Leftrightarrow false$ правило преобразования будет иметь вид:

$$right_{si} = right^1_{si} \,\&\, right^2_{si} \,\&\, ... \,\&\, right^n_{si}, \quad (5)$$

где $right^j_{si} \in e^j_{si}$.

Получаем новый список доступа: $L^5=\{E^5_s\}$

$E^5_s=\{E^5_{s1}, E^5_{s2}, ..., E^5_{sn}\}, E^5_{si}=(sid_{si}, right_{si}), \ \forall si \in P_u$;

8. Создаем список $L^6=\{E^6_s\}$ прав пользователей и групп с наибольшим приоритетом: $E^6_s=\{E^6_{s1}, E^6_{s2}, ..., E^6_{sn}\}, E^6_{si}=(sid_{si}, right^6_{si})$. Применим (6) $\forall E^5_{si} \in L^5$. Если булево выражение (6) истинно, тогда $E^5_{si} \to E^6_{si}$ и добавляется в L^6:

$$R'_{si} = !\exists r_{sj} > r_{si}, \quad (6)$$

где r_{si}, r_{sj} – приоритеты для объектов доступа si <=> uid, sj <=> uid.

9. Определяем значение логической функции соединения как:

$Conn_j(cid, proc(i,uid), proxy\_id, addr\_rec, addr\_snd, serv) = right^6_{s1} \,\&\, right^6_{s2} \,\&\, ... \,\&\, right^6_{sm} = right_{conn}$.

10. Определяем действующее правило:

$$\overline{Rule}_{conn} = \begin{cases} \text{if } (right_{conn} = true) \text{ then } run(accept); \\ \text{if } (right_{conn} = false) \text{ then } run(reject). \end{cases} \quad (7)$$

Если $right_{conn}=true$, то запрос на установление соединения $Conn_i$ считается действительным и соединение создается. В противном случае запрос отклоняется.

9. Метод формирования действующей политики

Политики есть наборы правил $\pi=\{R\}$. Если же имеем множество пользователей *{user}* и множество ресурсов *{resource}*, то

$$\pi = \{Rul_{user_i, resource_j}\} = \bigcup_{i=1}^{|users|} \bigcup_{j=1}^{|resources|} Rule_{user_i, resource_j}.$$

Если существуют ограничения на права E, то действующая политика будет сформирована из совокупности действующих правил.

Действующее правило вычисляем, применяя метод определения действующего правила для каждого пользователя, запрашивающего каждый из ресурсов. При этом действующая политика будет иметь вид:

$$\pi_D = \{\overline{\text{Rule}}_{\text{user}_i,\text{resource}_j}\}_{\forall \text{user}_i, \forall \text{resource}_j} = \\ = \bigcup_{i=1}^{|\text{users}|} \bigcup_{j=1}^{|\text{resources}|} \overline{\text{Rule}}_{\text{user}_i,\text{resource}_j} .$$

10. Пример формирования действующего правила

Приведем пример нахождения значения правила доступа для некоторой сети и запроса на соединение Reqv.

Предусловия. Пусть в сети существуют пользователи, объединенные в группы. Пользователям и группам присвоены приоритеты.

Пользователь A входит в группы C и E: P_A={A,1;B1;E,0}= {1,1;3,1;5,0}.

Пользователь B входит в группы C, D и F: P_B={2,2;3,1;4,1;6,1}={B,2;C,1;D,1;F,1}.

В сети заданы ресурсы: хосты с адресами mail.ru, www.mail.ru, хост инициатор 10.0.0.10 и сервис smtp. Для пользователей и групп заданы требования доступа к ресурсам.

Пользователь B, работая на хосте 10.0.0.10, пытается соединиться с mail.ru по smtp. При этом формируется запрос

Reqv_B=(cid, proc(i,uid), proxy_id, addr, addr, serv) = (1251, proc(12,B), 10.0.0.10, mail.ru, smtp).

Стратегия по умолчанию – доступ запрещен.

Требования доступа пользователей и групп заданы в следующем виде:

1. По умолчанию всем пользователям запрещен доступ к mail.ru.

2. Для группы C доступ ко всем хостам по SMTP разрешен.

3. Для пользователя B разрешен доступ к mail.ru по SMTP.

4. Для пользователя A запрещен доступ к www.mail.ru.

5. Пользователям группы C запрещен выход во внешнюю сеть с хоста 10.0.0.10.

По требованиям формируем список доступа (таблица):

L={t,E}={deny, E};

E ={E_1, E_2, E_3, E_4, E_5} – права доступа;

E_1=(sid_1, right_1, Conn_1)=(sid_1, right_1, (cid, proc(i,uid), proxy_id, addr_rec, addr_snd, serv)) =(*,deny,(*,*,mail.ru,*,*)),

E_2 =(C, allow, (*,*,* ,*,smtp)),

E_3 =(B, allow, (* , * , mail.ru, *,smtp)),

E_4=(A,deny,(*,*,www.mail.ru,*,*)),

E_5=(C,deny,(*,*,*, 10.0.0.10,*)).

E_1 – политика ресурса; {E_2, E_3, E_4, E_5} – политики пользователя.

Оперативное управление. Пользователь генерирует запрос Reqv_B и направляет его по сети. При этом Proxy-сервер должен определить – принять либо отклонить запрос.

1. При поступлении запроса Reqv_B на сервер контроля доступом сервер запрашивает маркер доступа пользователя с uid=2:

P_2={2,2;3,1;4,1;6,1}={B,2;C,1;D,1;F,1}.

2. Сравниваем элементы множества Reqv_B и E_i, если (3) выполняется, то помещаем E_i в L^1.

E_1 не удовлетворяет правилу (3), так как здесь права для ресурсов не включаются, а право E_1 регламентирует доступ к хосту с именем mail.ru для всех (sid=*) пользователей и групп.

E_2 удовлетворяет правилу (3), так как пользователь B входит в группу C, работает с mail.ru по smtp и право E_2 регламентирует доступ по smtp группы C.

E_3 удовлетворяет правилу (3), так как пользователь B соединяется по smtp к mail.ru и право E_3 регламентирует доступ пользователя B по smtp к mail.ru.

E_4 не удовлетворяет правилу (3) так как пользователь B сформировал запрос, а право E_4 регламентирует доступ пользователя A.

E_5 удовлетворяет правилу (3), так как пользователь B работает с хоста 10.0.0.10 и право E_3 регламентирует доступ пользователя B с хоста 10.0.0.10:

$$L^1 = \{E_2, E_3, E_5\}.$$

3. Формируем L^2 из L^1. Для этого выбираем из L^1 права для пользователя B и помещаем в E^2_{s1}. E^2_{s1} = E^2_2 ={E_3}.

Далее выбираем права для группы C и помещаем их в E^2_{s2}, и т.д.

В результате получаем $L^2 = \{E^2_s\}$, $E^2_s = \{E^2_{s1}, E^2_{s2}, \ldots, E^2_{sn}\}$, где si в данном случае есть идентификатор пользователя либо группы, т.е.

L^2 = {E^2_s}={E^2_2, E^2_3, E^2_4, E^2_6};

E^2_{s1} = E^2_2 ={E_3}- для пользователя B;

E^2_{s2} = E^2_3 = {E_2, E_5} – для группы C;

E^2_{s3} = E^2_4 = {$\emptyset$} – для группы D;

E^2_{s4} = E^2_6 = {$\emptyset$} – для группы F.

4. Создаем L^3, дополняя пустые политики из L^2 правом по умолчанию t: $E^3_{s4} = \{t\}, E^3_{s6} = \{t\}$.

L^3 = {{E_3},{E_2, E_5},{t},{t}}.

5. Формируем множество прав для ресурса E^r={E_1}, так как только в E_1 не определен объект доступа.

6. Формируем L^4, дополняя L^3 правами для ресурсов E^r_i. Для этого сравниваем поочередно все права для ресурсов E^r со всеми элементами E^3_{si}.

E_1 не включается в E^4_2, так как (addr_rec=mail.ru) О E_1 и у E_3 совпадают – значит E_3 является конкретизацией E_1.

E_1 включается в E^4_3, так как addr_rec у E_1 определен, а у E_2 и E_5 он общий.

E_1 включается в E^4_4 и E^4_6, так как (addr_rec=mail.ru) О E_1 определен, а у права по умолчанию t он общий.

В результате получаем $L^4 = \{\{E_3\},\{E_2, E_5, E_1\},\{t, E_1\},\{t, E_1\}\}$.

7. Получаем список $L^5=\{E^5_s\}$ объединением элементов внутри множеств E^4_{si}. В данном случае $L^5=\{E^5_s\}=\{E^5_2, E^5_3, E^5_4, E^5_6\}$.

$E^5_{s1} = E^5_2 = \{E_3\}$=(2,allow)-для пользователя B;

$E^5_{s2} = E^5_3 = \{E_2, E_5, E_1\}$=(3,allow && deny && deny) =(3,deny)– для группы C;

$E^5_{s3} = E^5_4 = \{t, E_1\}$=(4, deny && deny)– для группы D;

$E^5_{s4} = E^5_6 = \{t, E_1\}$=(6, deny && deny)– для группы F.

8. Создаем список $L^6 = \{E^6_s\}$ прав пользователей и групп с наибольшим приоритетом: $E^5_s = \{E^5_{s1}\} = \{E^5_2\} = \{E_3\}$.

9. Определяем значения логической функции $Conn_B$(cid, proc(i,uid), proxy_id, addr_rec, addr_snd, serv) = $Conn_B$(1251, proc(12,B), 10.0.0.10, mail.ru, smtp)= $right^4_{s1} = allow$.

10. В результате определяем действующее правило:

$$\overline{Rule_{conn}} = [\text{if (conn = allow) then run(accept)}].$$

Найденное действующее правило разрешает соединение по запросу $Reqv_B$. Пользователю B разрешается установление соединения.

№	E_i	sid	right	proxy_id	addr_rec	addr_snd	serv
1			Deny				
2	E_1	*	Deny	*	mail.ru	*	*
3	E_2	3	Allow	*	*	*	smtp
4	E_3	2	Allow	*	mail.ru	*	smtp
5	E_4	1	Deny	*	www.mail.ru	*	*
6	E_5	3	Deny	*	*	10.0.0.10	*

11. Пути дальнейшего развития предлагаемых методов и направления исследований

Предполагается расширить метод для контроля доступа за любыми ресурсами сети согласно общей информационной модели. Универсализация такого метода позволит определить семантику использования модели CIM с однозначной реализацией на множестве платформ.

Также планируется разработка алгоритма кэширования решений Proxy сервера для оптимизации работы метода. Необходимо описать конфликты, которые возникают при редактировании прав доступа пользователей и ресурсов, выработать правила их разрешения. Предполагается оптимизировать хранение и выборку правил доступа из списка доступа для сокращения времени работы метода формирования действующего правила.

12. Выводы

Впервые разработан метод формирования действующих политик, основанный на определении действующих правил доступа пользователей к ресурсам, путем вычисления логических выражений между элементами множеств ресурсов и объектов доступа с учетом заданных ограничений на связанные элементы этих множеств.

Оригинальность метода состоит в использовании новой семантики и в формировании логических выражений при определении правила доступа.

Научная новизна метода заключается во введении действующего правила как решения сервера контроля доступа на использование ресурса и основного элемента действующей политики при наличии ограничений на использование ресурсов. Осуществлено разделение прав на права ресурса (общие права) и права пользователей (уточняющие права).

Практическая значимость состоит в увеличении гибкости настроек средств контроля доступа в сети с упрощением перехода от требований к политикам менеджмента при внедрении данного метода.

Литература: 1. *Mark L. Stevens, Walter J. Weiss* "Policy based Management for IP networks" // Bell Labs technical journal. October – December 1999. C.75-93. **2**. Specification "CIM Core Policy Model" DSP1000, December, 2000, 56C. www.dmtf.org. **3.** Specification "CIM Policy Model" DSP1080, December, 2000, 67C., www.dmtf.org. **4** *Саенко В.И., Голубев А.С.* Метод формирования и описания политик доступа к ресурсам в компьютерной сети // Радиоэлектроника и информатика. 2004. №4. **5.** *Enhab S. Al-Shaer, Hamez H. Hamed* "Management and Translation of Filtering Security Policies" // IEEE. – 2003. №3. С. 56-70.

Поступила в редколлегию 01.11.2004

Рецензент: д-р техн. наук, проф.Путятин Е.П.

Саенко Владимир Иванович, канд.техн.наук, доцент, профессор каф. ИУС ХНУРЭ. Научные интересы: менеджмент компьютерных сетей, модели состояния и методы распределения ресурсов в компьютерных сетях. Увлечения и хобби: садоводство. Адрес: Украина, 61161, Харьков, пр. Ленина, 14, тел. 7021-415.

Голубев Александр Сергеевич, аспирант каф. ИУС ХНУРЭ. Научные интересы: технологии управления сетями. Увлечения и хобби: Java. Адрес: Украина, 61161, Харьков, пр. Ленина, 14, тел. 7021-415.