УДК 519.713

МЕТОД ФОРМИРОВАНИЯ И ОПИСАНИЯ ПОЛИТИКИ ДОСТУПА К РЕСУРСАМ В КОМПЬЮТЕРНОЙ СЕТИ

САЕНКО В.И., ГОЛУБЕВ А.С.

Рассматривается подход к решению проблем разделения ресурсов и контроля доступа пользователей в корпоративных сетях. Процесс формирования политик доступа декомпозируется на создание политик ресурса и политик пользователя в соответствии с методами глобального и локального управления.

1. Проблема менеджмента ресурсов компьютерных сетей

Сейчас практически все информационные системы используют компьютерную сеть в качестве транспортной среды передачи информации. Она позволяет множеству пользователей работать через программные приложения с одной и той же системой независимо от того, где они находятся. Сами приложения могут размещать свои компоненты на различных серверах и наравне с пользователями занимать ресурсы сети для передачи данных. Тенденции развития сетей таковы, что сколько бы дополнительных ресурсов не имела сеть, наступает момент, когда этих ресурсов становится недостаточно. В этих условиях возникает необходимость управления доступом к ресурсам на основе каких-то правил или требований. Сети, как и любая другая система, нуждаются в управлении. Однако особенности современных корпоративных сетей делают их управление весьма сложным. Требуется наличие специальных аналитических и информационных средств, позволяющих осуществлять принятие решений в сложных условиях неопределенности состояния сети.

Проблемой является разработка таких методов управления доступом к ресурсам, которые бы учитывали реальное функционирование сети и реальные технологии межпроцессного взаимодействия.

2. Анализ известных результатов исследований в области менеджмента сложных систем

Одной из последних тенденций в области управления сетями является использование специальных наборов правил, называемых *политиками* [1]. Политика содержит правила, обязательные для исполнения. Такие правила позволяют заранее программировать поведение активных элементов сети в случае чрезвычайных ситуаций. Например, при физическом повреждении кабеля трафик может перенаправляться через резервный физический канал.

Существует ряд стандартов в отношении политик. Таковыми, например, являются: CIM [2], DEN [3], WBEM [4]. Эти стандарты определяют общие концепции схемы данных, протоколы доступа, средства хранения политик. Задача таких стандартов – обеспечить интерфейсную часть для интеграции множества решений от различных производителей. Однако они практически не затрагивают особенностей реализации политик алгоритма принятия решений.

Методы, использованные при реализации средств менеджмента сети, являются собственностью создающих их компаний. Таким образом, внутренние оптимизированные механизмы работы с политиками в большинстве своём закрыты и являются коммерческой тайной. Рассматриваемые проблемы и задачи сегодня достаточно детально обсуждаются в научных статьях и на конференциях.

В частности, в [5, 6] обсуждаются методы представления политик в терминах объектов, а также возможности применения их в различных областях сетевого менеджмента. Также рассматривается метод баланса нагрузки на домен серверов. Был введен критерий загруженности сервера исходя из количества и типа задач, которые он выполнял.

В [7] рассматривалось применение политик для упрощения настройки брандмауэра. Здесь были освещены возможные случаи противоречий, возникающих в процессе редактирования, представлены способы выявления и разрешения конфликтов. Основные операции проводились с IP адресами отправителя и получателя, сами же пользователи не учитывались. Правила сетевого доступа в большинстве организаций принимаются на основе административных правил. Поэтому необходимо принимать решение о доступе, руководствуясь именно сведениями о пользователе.

Цель исследования состоит в разработке методов описания правил принятия решений в компьютерной сети при управлении доступом пользователя к ресурсам.

3. Описание объекта исследования

Пусть имеется некоторая корпоративная компьютерная сеть *Net* с централизованным администрированием. Это значит, что распределение ресурсов осуществляется в соответствии со строго определенными правилами для всей сети. Пусть имеется общий ресурс *Res*, например, логический канал доступа к Интернет. Доступ осуществляется через Proxy-сервер. Пусть логический канал доступа к Интернет представлен несколькими физическими каналами N. Для повышения надежности внешние каналы имеют разную природу (кабель, спутник) и различные характеристики пропускной способности и задержки. Все внешние каналы подключены к одному шлюзу – Proxy-серверу.

В сети активны некоторое множество пользователей M={*Users*} и групп G={Groups}, в которые пользователи могут быть объединены (рисунок).

Пользователи через программные приложения получают доступ к каналу Интернет. Считаем, что каждый пользователь создает в процессе соединения некоторую нагрузку на сеть. Каналы имеют ограниченную полосу пропускания. Суммарная нагрузка

на сеть больше, чем пропускная способность каналов. В сети наблюдается дефицит ресурсов.

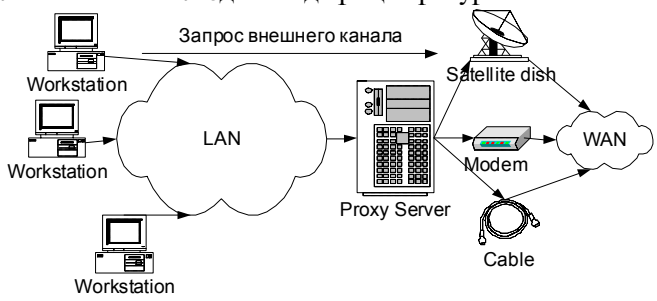

Схема доступа пользователя к ресурсам

4. Постановка задачи

Пусть есть компьютерная сеть. В сети присутствуют процессы, порождающие информационные потоки в результате обмена информацией приложений пользователей и ресурсов Интернет. Потоки проходят через сервер Proxy, образуя соединения $Conn_j$. Процессы обладают определенными правами, соответствующими правам пользователей acc(uid). Права пользователя устанавливаются в соответствии с общими правилами распределения ресурсов сети.

Требуется сформировать метод и определить семантику задания правил, по которым Proxy-сервер смог бы осуществлять контроль и управление доступом пользователей к фиксированным внутренним ресурсам сети в виде соединений с внешними ресурсами.

5. Описание семантики формирования правил доступа к ресурсам сети

Для решения задачи определим несколько семантических понятий.

Компьютерная сеть представляется в виде множества ресурсов *{Res}* и процессов *{proc(i)}*.

Функционирование компьютерной сети представляется как отношение между процессами и ресурсами.

Определение 1. *Ресурс* – информационный объект, абстрактный элемент сети, используемый как класс со свойствами: имя (идентификатор – *Res*), тип ресурса, технические параметры Res_i={type,{Param}}, где type – тип, параметр $Param_i$={name,value} – имеет имя и значение. Экземпляры класса характеризуют конкретный ресурс. Например, *трафик-ресурс* - это ресурс, требуемый для обеспечения передачи данных между двумя приложениями (процессами) в компьютерной сети.

Определение 2. *Трафик* – поток данных f_j между двумя узлами (ws_k,ws_r), проходящий по некоторому пути. Измеряется в *bps*.

Определение 3. *Путь* – набор связанных в цепочку узлов (ws_k, ws_k, ws_{k+1}, ws_{k+2},..., ws_r). Так как внешние соединения подключены к Proxy-серверу, то один из элементов пути ws_i будет соответствовать Proxy_id.

Процессы связаны с логическими объектами в сети – пользователями (или системными объектами, выступающими в роли системных пользователей).

Определение 4. *Пользователь* – информационный объект, абстрактный элемент сети, используемый как класс со свойствами: имя (идентификатор - uid), описание прав доступа к ресурсам, ссылки на права доступа к ресурсам. Экземпляры класса характеризуют конкретных пользователей и конкретные права доступа к ресурсам со стороны процессов, порождаемых пользователем.

Определение 5. *Группа* – информационный объект, элемент сети, используемый как класс со свойствами: имя группы, имена пользователей, описания прав доступа к ресурсам, ссылки на права доступа к ресурсам. Экземпляры этого класса объединяют несколько пользователей и характеризуют набор правил, определяющих права пользователей по отношению к ресурсам.

В сети задано множество пользователей $u_j \in M$ и множество групп $g_j \in G$. Каждый из пользователей и групп однозначно определяется своим ID $(u \to uid, g \to gid)$. Каждый пользователь u_i может входить в некоторое подмножество G' групп $u \in G'_u$, при этом $G' \subset G$. Так как задача решается безотносительно платформы, то мы не знаем правила включения групп и пользователей друг в друга. Однако для упрощения будем считать, что

1) группы и пользователи могут входить в произвольное число групп:

$$\forall i, \forall j : u_i \subset g_1, u_i \subset g_2, ..., u_i \subset g_{a1};$$
$$g_j \subset g_1, g_j \subset g_2, ..., u_j \subset g_{a2},$$
$$g_j \in G, u_i \in M;$$

2) пользователи не могут включать пользователей либо группы:

$$u_i \not\subset u_j, \forall i, \forall j, i \neq j, u_i \in M;$$
$$g_i \not\subset u_j, \forall i, \forall j, u_i \in M, g_j \in G;$$

3) группы включаются так, чтобы не организовать цикла:

$$\forall l : g_1 \subset g_2 \subset ... \subset g_1, g_1 \not\subset g_{(l-a)}, a = 1..(l-1).$$

Определение 6. *Соединение* – это информационный объект, элемент сети, используемый как класс со свойствами: имя (идентификатор – **$Conn_j$**), имя компьютера, с которого устанавливается соединение - **(cid),** имя процесса с инициирующего соединение **(proc(i,uid)),** права процесса, наследованные от пользователя **(acc(uid)),** Proxy-сервер, через который производится соединение **(Proxy_id),** адрес или имя ресурса, с которым производится соединение **(addr),** тип сервиса, в рамках которого производится соединение **(serv).** Экземпляры **соединения** являются элементами сети, отражающими факт того, что в текущий момент некоторый процесс, заданный идентификатором компьютера cid и правами пользователя acc(uid), создает трафик

(f_j) (поток данных), характеризуемый компьютером процесса cid, граничным шлюзом (Proxy-server, вектор направления трафика), адресом требуемого ресурса (addr) и видом сервиса (serv).

Соединение –

$$Conn_j(cid, proc(i,uid), acc(uid), Proxy_id, addr, serv). \quad (1)$$

Соединение, как объект, отражает текущее состояние сети и ресурсов. Используется для реализации методов мониторинга и оперативного управления состоянием компьютерной сети.

Определение 7. *Запрос* $Reqv_j$ – набор пакетов, образующих транзакцию, передаваемых между двумя узлами и связанных с требованием выполнения какого-либо действия в момент t. Запрос на доступ к соединению $Conn_i$ представляется в виде $Reqv_j = (T, Conn_i)$, где T- дискретное время.

Определение 8. *Политика* – набор правил, в соответствии с которыми выбираются определенные действия при выполнении некоторых условий стратегии сети.

Определение 9. *Стратегия* – целевые функции сети, определяющие требования и критерии функционирования сети. Стратегия распределения ресурсов определяет требования и правила к принятию решений по доступу процессов к ресурсам.

Определение 10. *Маркер доступа* – это множество элементов групп, в которые входит пользователь прямо или косвенно, элемент личного приоритета пользователя и идентификатор. Маркер доступа описывает пользователя.

Маркер доступа: $P = (\{u_i, r_i\}, \{g_1, r_1\}, \{g_2, r_2\} \ldots \{g_l, r_l\})$, если $u_i \subset g_k, k = 1..l, u_i \in M, g_k \in G$, r_i – приоритеты пользователя и групп, M – множество пользователей сети, G – множество групп в сети.

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

$$P_u = \{\{uid_i, r_i\}, \{gid_u^1, r_u^1\}\{gid_u^2, r_u^2\}, \ldots, \{gid_u^h, r_u^h\}\}, \quad (2)$$

где $h = |G'_u|, u \in m, uid_u \leftrightarrow u, gid_u^h \leftrightarrow g, u \subset g, u = 1..h$,

G'_u – набор групп, в которые входит пользователь u; uid_u – идентификатор пользователя u; gid^h_u – идентификатор группы, в которую входит пользователь u, u=1...h.

Определение 11. *Список доступа* – множество элементов, определяющее права для каждого соединения в компьютерной сети.

Каждый элемент списка будет разрешать либо запрещать генерацию трафика некоторому пользователю или группе. Списки доступа имеют такую структуру: $L_k = \{t, E\}$, где k – целое значение, соответствующее типу ресурса в рамках некоторой классификации; t – запись, регламентирующая доступ по умолчанию (для всех); E – множество записей для некоторого пользователя либо группы, $G \cup M$. Доступ по умолчанию регламентируется самой первой записью.

Запись t содержит только action′ – доступ по умолчанию. Данная запись нужна для определения политики по умолчанию для некоторого вида трафика.

Определение 12. *Право доступа* $E_i = \{sid_i, action_i, Res_i\}$ – структура, состоящая из элементов $sid_i \in \{uid, gid\}$ – идентификатор пользователя либо группы, $action \in \{allow, deny\}$.

Определение 13. *Правило доступа* – функция rule(E(uid)), принимающая значение rule ={allow, denay}в зависимости от прав доступа пользователя E(uid) к ресурсу Res_i в структуре $E_i = \{uid, action_i, Res_i\}$.

6. Описание стратегий распределения ресурсов

По начальному условию рассматриваемая компьютерная сеть имеет централизованную политику администрирования и единые правила распределения ресурсов. Считаем, что в сети обобщенные правила представляют некоторую стратегию. Стратегию будем представлять в виде вербального описания главных условий описания правил распределения ресурсов. В большинстве своем стратегии зависят от организационных особенностей предприятия. Стратегии ресурсов выбираются для формирования политик при дефиците ресурсов.

Условия использования каналов доступа к ресурсам:

– каналы доступа разрешается загружать не более, чем заранее выделенная полоса пропускной способности;

– число пользователей, использующих канал, определяется суммарной нагрузкой, создаваемой ими.

Стратегия A. Пользователи получают доступ к ресурсам без ограничений на полосу пропускной способности, при равных приоритетах, по принципу обычной очереди с полным обслуживанием за время сеанса.

Стратегия B. Пользователи получают доступ к ресурсам без ограничений на полосу пропускной способности, при разных личных приоритетах, по принципу обычной очереди с полным обслуживанием за время сеанса. Если в очереди имеется пользователь с более высоким приоритетом, то пользователь с низким приоритетом блокируется и переводится в конец очереди, а пользователь с высоким приоритетом получает доступ к ресурсу.

Стратегия C. Пользователи получают доступ к ресурсам без ограничений на полосу пропускной способности, при разных групповых приоритетах, по принципу обычной очереди с полным обслуживанием за время сеанса. Если в очереди имеется пользователь с более высоким групповым приоритетом, то пользователь с низким приоритетом блокируется и переводится в конец очереди, а пользователь с высоким приоритетом получает доступ к ресурсу. В этом случае образуются специальные группы с разными возможностями доступа к сети.

Стратегия D. Пользователи получают доступ к ресурсам без ограничений на полосу пропускной

способности, при разных групповых и личных приоритетах, по принципу обычной очереди с полным обслуживанием за время сеанса. Если в очереди имеется пользователь с более высоким групповым приоритетом, то пользователь с низким приоритетом блокируется и переводится в конец очереди, а пользователь с высоким приоритетом получает доступ к ресурсу. Это справедливо при сравнении пользователей, входящих в разные группы, и для пользователей, входящих в одну и ту же группу.

Остальным пользователям отказано в доступе.

7. Анализ использования предложенной семантики

По маркеру доступа невозможно определить взаимосвязь между группами, либо в какие группы входит пользователь непосредственно, а в какие косвенно. Здесь пользователь может входить прямо и косвенно в группы, включающие друг друга:

$$u_i \subset g_j, u_i \subset g_k; g_j, g_k \subset G, u_i \subset M .$$

Такая схема включения нежелательна, так как при установке правил возможно возникновение логического конфликта, который трудно обнаружить. Это обстоятельство похоже на ситуацию, при которой на предприятии один человек занимает две должности. При этом одна должность подчинена другой. Получается, что одна персона подчиняется сама себе и имеет в одно и то же время разные полномочия. При реализации такой схемы возможны технические конфликты в случае, если запрещающие правила имеют более высокий приоритет, чем разрешающие.

8. Метод менеджмента трафик-ресурсов на основе политик

За основу примем концепцию, при которой следует определить отношения между ресурсами и пользователями, выражающиеся в виде создания экземпляров “соединение” (информационных объектов).

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

Представленная задача сводится к задаче ситуационного управления, когда на основании некоторых условий выбирается известное действие.

Предлагается рассматривать две стратегии. Одна стратегия для ресурсов, т.е. для описания прав доступа к конкретному ресурсу, другая – для описания прав пользователя (на стороне пользователя или сервера аутентификации).

Стратегия для ресурса St_Resource. Для каждого ресурса определяются логические объекты, пользователи и группы, которые могут использовать данный ресурс или которым запрещено его использование (в зависимости от политики по умолчанию).

Стратегия для пользователя St_Users. Для каждого пользователя определен перечень ресурсов, к которым разрешен доступ.

В соответствии со стратегиями предлагается сформировать следующие политики:

Политика серверов $\mathbf{\pi}_{server}$. Набор правил, определяющих доступ к конкретному серверу (например, Proxy) в соответствии со стратегией *St_Resource*.

Политика сервисов $\mathbf{\pi}_{prot}$. Набор правил, определяющих право работы в рамках определенного сервиса или протокола в соответствии со стратегией *St_Resource*.

Политика адресов $\mathbf{\pi}_{name}$. Набор правил, определяющих право работы с определенным ресурсом, заданным известным адресом или именем в соответствии со стратегией *St_Resource*. Используется только для известных заранее имен для запрета доступа.

Политика пользователя $\mathbf{\pi}_{user}$. Набор правил, определяющих доступ к ресурсам для конкретного пользователя в соответствии со стратегией *St_Users*.

Для того чтобы упростить формирование политик, часто используются методы, основанные на применении политики по умолчанию. Предлагается также использовать такой подход. Прежде всего определим стратегии по умолчанию:

Стратегия St_+. – по умолчанию в сети разрешен доступ ко всем ресурсам и для всех пользователей. Если политика в конкретном случае не определена, то доступ считается открытым.

Стратегия St_-. – по умолчанию в сети запрещен доступ ко всем ресурсам и для всех пользователей. Если политика в конкретном случае не определена, то доступ считается закрытым.

Соответственно формируются политики.

Существует два типа политик:

1) Разрешено все, что не запрещено, т.е. по умолчанию все разрешено: action′=allow, при этом для всех пользователей и групп, которые явно не указаны в списке доступа, доступ разрешен:

$$\text{IF action}'_k = \text{allow THEN}$$
$$(\text{IF sid}_S \notin L_k \text{ THEN action}_{S,k} = \text{allow}),$$

где $action'_k$ – возможность доступа к ресурсу k по умолчанию; sid_s – идентификатор группы либо пользователя s; L_k – списки доступа для ресурса k; $action_{s,k}$ – разрешение доступа к ресурсу k для пользователя либо группы s.

2) Разрешено то, что разрешено, т.е. по умолчанию запрещено все: action′=deny, при этом для всех пользователей и групп, которые явно не указаны в списке доступа, доступ запрещен:

$$\text{IF action}'_k = \text{deny THEN}$$
$$(\text{IF sid}_S \notin L_k \text{ THEN action}_{S,k} = \text{deny}),$$

где action′$_k$ – возможность доступа к ресурсу k по умолчанию; sid_s – идентификатор группы либо пользователя s; L_k – списки доступа для ресурса k; $action_{s,k}$ – разрешение доступа к ресурсу k для пользователя либо группы s.

Если есть пользователи, которые имеют привилегированное положение, это задается в политиках π_{user}.

Формируется дополнительная группа пользователей, которые смогут получить доступ, если канал будет в это время свободен (статистическое мультиплексирование). Создание такой группы осуществляется на основе личных приоритетов, заданных в рамках маркера доступа.

Активность работы пользователя определяется двумя фазами: запросом на соединение и собственно работой с ресурсом. Работа с ресурсом возможна после получения прав на создание соединения с требуемым ресурсом.

Реализацию метода можно разделить на несколько этапов: *подготовительный, реализация политик, оперативное управление.*

Пусть имеется компьютерная сеть и определены условия управления ресурсами, как было описано выше.

Пусть для сети определена некоторая стратегия распределения ресурсов и используется принцип комбинированного управления доступом (на основании задания прав для пользователя и для групп).

Таким образом, метод менеджмента сводится к следующему.

Подготовительный этап:

– формируются стратегии менеджмента доступа к трафик-ресурсам;

– формируются цели менеджмента и целевые функции (при необходимости).

Реализация политик доступа:

– устанавливаются политики по умолчанию;

– вводятся приоритеты;

– для регулирования доступа пользователей к внешним каналам необходимо ввести для каждого типа ресурса список доступа;

– формируются политики ресурсов;

– формируются политики пользователей.

Оперативное управление:

– обрабатываются запросы пользователей;

– выявляются действительные права пользователя по отношению к требуемому ресурсу;

– принимаются решения по созданию требуемого объекта “соединение”.

Необходимость представления общей сетевой политики в виде политик пользователя и ресурсов обусловлена тем, что сеть представляет собой сложную систему, и выбирать стратегию, связанную только с доступом к ресурсам, т.е. для каждого ресурса предусмотреть все ситуации – нецелесообразно. Эффективным представляется в политике ресурса задавать общие условия, а в политике пользователя – указывать конкретные ограничения (временные).

В этом случае мы получаем следующие методы управления:

– *метод глобального управления* состоянием ресурсов, основанный на предварительном распределении прав доступа к разным ресурсам и создании политик доступа к ресурсам. Политики создаются для всех ресурсов, необходимых для обеспечения существования потока;

– *метод локального управления* состоянием ресурсов, основанный на предварительном распределении прав доступа к разным ресурсам для каждого пользователя в отдельности. Политики создаются для каждого пользователя;

– *метод оперативного управления* состоянием ресурсов, основанный на контроле за объектами “соединение” и определении их статуса в текущий момент. Дополнительно используются политики пользователя и их приоритеты.

9. Метод описания прав доступа для политик

На основании сказанного выше предлагается метод описания политик.

Известно, что для управления доступом к ресурсам в сети могут быть использованы три метода: метод доступа, основанный на определении прав для процессов; метод доступа, основанный на определении прав для пользователей, метод доступа, основанный на определении прав для групп пользователей.

Будем использовать комбинированный метод управления доступом к ресурсам, основанный на определении прав доступа групп и пользователей.

Функция аутентификации возложена на операционную систему. Таким образом, личности субъектов, работающих в сети, подтверждены внешними по отношению к задаче средствами. После аутентификации каждый пользователь получает маркер доступа. Маркер доступа используется приложениями и операционной системой при проверке доступа пользователя к разделяемым ресурсам.

10. Пример описания политик

Приведем пример описания политик доступа для некоторой сети.

Подготовительный этап:

Примем за основу стратегию A. Стратегия по умолчанию – доступ разрешен St_+. Пусть в сети существуют пользователи, объединенные в группы, приоритет не используется $r_i = 0$:

$$P_A=(\{ui,ri\},\{g1,r1\},\{g2,r2\}\{gl,rl\})=(1,0,3,0,4,0),$$

$$P_B=(2,0,4,0,5,0,6,0,7,0).$$

Реализация политик:

В соответствии со стратегией определим политики. Сформулируем основные требования для политик:

1. π_{conn}: закрыть доступ всем пользователям для POP3 протокола, группе G – доступ к ресурсу каналов;

2. π_{user}: пользователю A закрыть доступ к хосту yahoo.com и по протоколу HTTP к ресурсу.

В соответствии с политиками создаем список доступа для соединений, использующих ресурс каналов:

$L_k=\{t,E_s\}=\{St_+, E_s\}=\{allow, E\}$;

$E=\{E_1, E_2, E_3, E_4\}$;

$E_1=\{sid_1, action_1, Conn_1\}=\{sid_1, action_1, (cid, proc(i,uid),acc(uid), Proxy_id, addr, serv)\} = \{*,deny,(*,*,*,192.168.2.255,*,pop3)\}$,

$E_2 = \{G, deny, (*,*,*,192.168.2.255,*,*)\}$,

$E_3 = \{A, deny, (*, *, *, 192.168.2.255, yahoo.com,*)\}$,

$E_4 = \{A,deny,(*,*,*,192.168.2.255, *,HTTP)\}$.

В таблице приведены значения для указанных выражений.

№	Sid	Action	Cid	Proc	Acc	Proxy_id	Addr	Serv
1		Allow						
2	*	Deny	*	*	*	192.168.2.255	*	pop3
3	7	Deny	*	*	*	192.168.2.255	*	*
4	1	Deny	*	*	*	192.168.2.255	yahoo.com	*
5	1	Deny	*	*	*	192.168.2.255	*	HTTP

Оперативное управление:

Пусть имеются запросы $Reqv_1$ и $Reqv_2$ на следующие соединения:

$Conn_j$(cid, proc(i,uid),acc(uid), Proxy_id, addr, serv)= $=Conn_1$ (1, proc(12, 1),acc(1), 192.168.2.255, yahoo.com, HTTP)=$Conn_1$ (1, 1282,0, 192.168.2.255, yahoo.com, HTTP);

$Conn_2$ (2, proc(14, 2),acc(2), 192.168.2.255, msdn.com, HTTP)= $Conn_2$ (2, 1424,0, 192.168.2.255, msdn.com, HTTP).

Соединение $Conn_1$ инициировано пользователем A с идентификатором 1, Proxy-сервер – 192.168.2.255, соединение с yahoo.com по HTTP, работаем без приоритета 0.

Соединение $Conn_2$ инициировано пользователем B с идентификатором 2, Proxy-сервер – 192.168.2.255, соединение с msdn.com по HTTP, работаем без приоритета 0.

По приходу запроса Proxy-сервер оборвет оба соединения. Достаточным условием для отказа в доступе к ресурсу является в первом случае адрес запрашиваемого ресурса – yahoo.com, а во втором то, что пользователь входит в группу G.

11. Пути дальнейшего развития предлагаемых методов и направления исследований

Предполагается расширить метод на условия, когда возникают противоречия в политиках при выборе конкретного действия, и рассмотреть возможность алгебраической связи параметров политик с целевыми функциями. Универсализация такого описания позволит использовать его при решении задач контроля доступа к разделяемым ресурсам сети.

Необходимо описать правила для контроля доступа пользователей к внешним каналам. Нужно определить схему данных для политик, а также метод доступа и тип хранилища данных.

При этом существуют требования к гибкости настроек сервера, простоте создания, редактирования, хранения и однозначности интерпретации семантики правил политик.

12. Выводы

Предложены усовершенствованные методы политик доступа пользователя к ресурсам, основанные на новых семантических концепциях логических объектов сети, отличающиеся простотой реализации и позволяющие построить эффективные процедуры принятия решений для узловых серверов.

Научная новизна методов состоит в формировании независимых политик доступа для ресурса и пользователя, возможности перехода от стратегий к политикам доступа.

Практическая значимость состоит в повышении эффективности работы алгоритмов формирования разрешения доступа к ресурсу при внедрении данных методов.

Существующие стандарты, а также узконаправленные реализации информационной модели политик не затрагивают процессы создания политик, перехода от требований и стратегий к реализации.

Реализация и внедрение данных методов обеспечит повышение гибкости настроек благодаря увеличению количества критериев фильтрации запросов разделяемых ресурсов.

Литература: 1. *Mark L. Stevens, Walter J. Weiss* "Policy based Management for IP networks" // Bell Labs technical journal. October – December, 1999. P.75-93. **2.** www.dmtf.org, Specification "CIM Core Policy Model May" 1000, December, 2000. 244 p. **3.** www.dmtf.org, Specification "DMTF LDAP Schema for the CIM V2.5 Core Information Model" DSP0100, May 8, 2000. 65 p. **4.** www.dmtf.org Specification "CIM Operations over HTTP", DSP0200 August 11th, 1999. 50 p. **5.** *Denish C. Verma, Tomas J Wasron.* Simplifying Network Administration Using Policy-Based Management // IEEE Network. March -April 2002. №3. P. 20-26 **6.** *Ashfaq Hossain, Houshing F. Shu, Charles R. Gasman.* Policy Based Network Load Management // Bell Labs technical journal. October – December 1999. P.95-107. **7.** *Enhab S. Al-Shaer, Hamez H. Hamed.* Management and Translation of Filtering Security Policies // IEEE. 2003. №3. P. 56-70.

Поступила в редколлегию 09.07.2004

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

Саенко Владимир Иванович, канд. техн. наук, доцент, профессор кафедры ИУС ХНУРЭ. Научные интересы: менеджмент компьютерных сетей. Увлечения и хобби: садоводство. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 7021-415.

Голубев Александр Сергеевич, студент ХНУРЭ. Научные интересы: технологии управления сетями. Увлечения и хобби: Java. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 7021-415.