Network Working Group
Request for Comments: 2753
Category: Informational

R. Yavatkar
Intel
D. Pendarakis
IBM
R. Guerin
U. Of Pennsylvania

January 2000

Модель контроля доступа на основе правил

A Framework for Policy-based Admission Control

Статус документа

В этом документе представлена информация для сообщества Internet. Документ не задает какого-либо стандарта Internet и может распространяться без ограничений.

Авторские права

1. Введение

Рабочие группы IETF, такие как Integrated Services[1] (int-serv) и RSVP [1] подготовили расширения архитектуры IP и модели обслуживания «по возможности» (best-effort), позволяющие приложениям и конечным пользователям запрашивать определенное качество (уровень) обслуживания от сети в дополнение к современным услугам IP best-effort. Недавние результаты рабочей группы Differentiated Services[2] также направлены на определение механизмов поддержки агрегатов услуг QoS[3]. Модель int-serv для этих новых услуг требует явной сигнализации требований QoS от конечных точек и обеспечения восприятия и управления трафиком на маршрутизаторах с интегрированным обслуживанием. Предложенные стандарты для RSVP [RFC 2205] и интегрированных услуг [RFC 2211, RFC 2212] являются примерами нового протокола организации резервирования и новых определений сервиса, соответственно. В модели int-serv некоторые потоки данных получают предпочтительное обслуживание по сравнению с другими потоками - компоненты управления восприятием (admission control) принимают во внимание лишь запросы ресурсов со стороны резервирующего и доступные возможности, но не принимают запросы QoS. Однако механизмы int-serv не включают важных аспектов управления восприятием - сетевые администраторы и сервис-провайдеры должны быть способны отслеживать, контролировать и форсировать использование ресурсов и услуг на основе правил, выводимых из таких критериев, как отождествление пользователей и приложений, потребности в пропускной способности, день недели, время суток. Механизмы diff-serv тоже должны принимать во внимание правила, включающие такие критерии, как отождествление пользователей, точки входа и т. д.

В этом документе определена схема управления на основе правил для решений по контролю доступа. В частности, документ посвящен управлению доступом на основе правил с использованием RSVP в качестве сигнализации QoS. Несмотря на то, что основное внимание уделено контролю восприятия на основе RSVP, в документе очерчена модель, способная обеспечить контроль восприятия в другом контексте QoS. Утверждается, что контроль на основе правил должен быть применим к разным типам и качеству услуг, предлагаемых в одной сети и цель состоит в рассмотрении таких решений при наличии возможности.

В разделе 2 приведены определения основных терминов. В разделе 3 указан список требований и целей механизмов, применяемых для контроля доступа и обеспечения лучшего QoS. Затем очерчены элементы архитектуры модели (раздел 4) и описана функциональность каждой компоненты. В разделе 5 приведены примеры правил, возможные варианты и поддержка политики для этих вариантов. В разделе 6 заданы требования к протоколу «клиент-сервер» для коммуникаций между сервером правил (PDP) и клиентом (PEP), а также оценена пригодность имеющихся протоколов.

2. Терминология

Ниже приведены определения используемых в документе терминов.

Administrative Domain - административный домен
Набор сетей с единым административным управлением, собранных в соответствии с административными целями.

Network Element или Node - элемент сети или узел
Маршрутизаторы, коммутаторы, концентраторы служат примерами сетевых узлов. Это элементы, где должны приниматься и исполняться решения о распределении ресурсов. Маршрутизатор RSVP, выделяющий часть канальной емкости (или буферов) для конкретного потока и гарантирует получение доступа к зарезервированным ресурсам лишь разрешенным потокам, служит примером элемента, представляющего интерес в этом контексте.
В этом документе термины «маршрутизатор», «элемент сети» и «узел сети» используются взаимозаменяемо, но все они должны рассматриваться как элементы сети.

QoS Signaling Protocol - сигнальный протокол QoS
Протокол сигнализации, передающий запросы контроля доступа к ресурсу, например, RSVP.

Policy - политика (правила)
Набор правил и услуг, где правила определяют критерии доступа и использования ресурса.

[1]Интегрированные услуги.
[2]Дифференцированные услуги.
[3]Quality of Service - качество обслуживания.

Policy control - проверка политики
Применение правил для определения возможности предоставления доступа к конкретному ресурсу.

Policy Object - объект политки
Содержит связанную с политикой информацию (такую как элементы политики) и передается в запросах и откликах, относящихся к решениям о доступе к ресурсу.

Policy Element - элемент политики
Часть элемента политики, содержащая единицу информации, требуемой для оценки правил политики. Один элемент политики может передавать идентификацию пользователя или приложения, а другой - свидетельсва пользователя или данные банковской карты. Предполагается, что сами элементы политики не зависят от используемого сигнального протокола.

Policy Decision Point (PDP) - точка принятия решений в политике
Место, где принимается решение в политике доступа.

Policy Enforcement Point (PEP) - точка исполнения решений политики
Место, где реально испольняется решение политики доступа.

Policy Ignorant Node (PIN) - игнорирующий политику узел
Сетевой элемент, который явно не поддерживает политику контроля доступа, с использованием описанных здесь механизмов.

Resource - ресурс
Нечто ценное (нужное) в сетевой архитектуре, доступ к которому предоставляется на основе критериев политики. Примерами ресурсов могут служить буферы в маршрутизаторах и пропускная способность интерфейсов.

Service Provider - сервис-провайдер
Контролирует сетевую инфраструктуру и может отвечать за учет и оплату услуг.

Soft State Model - модель “мягких” состояний
Soft state представляет собой вариант модели с учетом состояний, которые истекают через некоторое время после установки в PEP или PDP. Это способ автоматического удаления состояний при наличии отказов коммуникаций или сетевых элементов. Например, RSVP применяет такую модель для установки состояний резерва на сетевых элементах в пути потока данных через сеть.

Installed State - установленное состояние
Новый и уникальный запрос от PEP к PDP, который должен удаляться явно.

Trusted Node - доверенный узел
Узел в границах административного домена (AD), который считается доверенным в том смысле, что запросы управления доступом от этого узла не обязательно требуют решения PDP.

3. Контроль восприятия на основе правил - цели и требования

В этом разделе описаны цели и требования для механизмов и протоколов, разработанных для обеспечения контроля доступа на основе правил путем принятия решений.

Политика и механизмы
Важно отметить, что модель не включает какого-либо обсуждения поведения конкретной политики и не требует применения конкретных правил. Вместо этого схема описывает элементы архитектуры и механизмы, требуемые для поддержки различных вариантов политики.

RSVP
Должны быть разработаны механизмы для выполнения требований контроля доступа на основе правил, предназначенные для решения задачи резервирования пропускной способности с использованием RSVP в качестве сигнального протокола. Однако цель заключается лишь в том, чтобы разрешить применение этой модели для контроля доступа, включающего другие типы ресурсов и услуги QoS (например, Diff-Serv).

Поддержка вытеснения
Разрабатываемые механизмы должны включать поддержку вытеснения, с помощью которого можно удалять ранее установленные состояния, заменяя их новыми запросами контроля доступа. Например, в случае RSVP вытеснение включает возможность удалить один или несколько установленных резервов для освобождения ресурсов в соответствии с новым запросом на резервирование.

Поддержка разных стилей политики
Разрабатываемые механизмы должны поддерживать множество правил и конфигураций политики, включая двухсторонние и односторонние соглашения об обслуживании, а также правила, основанные на указании относительного приоритета. В общем случае определение и настройка жизнеспособной политики является обязанностью поставщика услуг.

Предоставление информации для мониторинга и учета
Должны обеспечиваться механизмы для мониторинга состояния политики, использования ресурсов и обеспечения информации о доступе. В частности, требуются механизмы предоставления информации о доступе и использовании, которая может применяться для учета и оплаты услуг.

Устойчивость к отказам и восстановление
Разработанные на основе этой модели механизмы должны включать обеспечение отказоустойчивости и восстановление при отказах, таких как отказы PDP, нарушение связи, включая разделение сети (и последующее слияние), отделяющее PDP от связанных PEP.

Поддержка узлов PIN
Поддержку описанных здесь механизмов не следует делать обязательной на каждом узле сети. Основанный на правилах контроль доступа может выполняться на части узлов, например, на границе административного домена. Эти узлы будут доверенными с точки зрения узлов PIN в этом административном домене.

Расширяемость
Одним из важных требований к механизмам управления политикой является возможность расширения. Эти механизмы должны быть расширяемыми по меньшей мере как RSVP с точки зрения поддержки множества потоков и сетевых узлов на пути потока. В частности, расширяемость должна учитываться при указании поведения по умолчанию при слиянии объектов политики данных и слияние не должно приводить к дублированию элементов или объектов политики. Имеется несколько важных с точки зрения расширяемости областей для управления политикой с помощью RSVP. Во-первых, не от каждого узла инфраструктуры, знающего о политике, ожидаются контакты с удаленной точкой PDP, поскольку это может приводить к значительным задержкам при проверке запросов, которая должна выполняться поэтапно. Во-вторых, RSVP может резервировать ресурсы для множества

потоков и это предполагает, что модель управления политикой должна быть способна обслуживать особые требования больших групповых потоков. Таким образом, архитектура управления политикой должна быть расширяемой не хуже RSVP, исходя из таких факторов, как размер сообщений RSVP, время обслуживания запроса RSVP, время локальной обработки запроса на узле и локальная память, расходуемая узлом.

Вопросы безопасности и атак на службы

Архитектура управления политикой должна быть защищена с учетом приведенных ниже аспектов. Во-первых, предлагаемые в рамках модели механизмы должны минимизировать угрозы хищения данных или отказов в обслуживании. Во-вторых, они должны гарантировать, что объекты (такие как PEP и PDP), участвующие в управлении политикой могут проверять отождествление друг друга и организовавыть доверенные отношения до начала взаимодействия.

4. Элементы архитектуры

Двумя основными элементами урхитектуры управления политикой являются точки применения правил (PEP) и точки принятия решений (PDP). На рисунке 1 показана простая конфигурация, включающая эти элементы. PEP являются компонентами узлов сети, PDP - удаленным объектом, который может размещаться на сервере политики. PEP представляет компоненту, которая всегда работает на осведомленном о политике узле и в ней исполняются принятые решения политики, которые принимаются в основном на PDP. Сама точка PDP может использовать дополнительные механизмы и протоколы для обеспечения дополнительных функций, таких как проверка подлинности пользователей, учет, хранение правил и т. п. Например, PDP может использовать службу каталогов LDAP для хранения и поиска правил [6]. В документе не рассматриваются эти дополнительные механизмы и протоколы, в также их применение.

Основное взаимодействие между компонентами начинается с PEP. Точки PEP будут получать уведомления или сообщения, требующие принятия решений. На основе таких событий PEP создает запрос для принятия решения и передает его PDP. Запрос управления политикой от PEP к PDP может содержать один или множество элементов политики (инкапсулируются в один или множество объектов политики) в дополнение к данным управления доступом (таким, как спецификация потока или запрос пропускной способности) из исходного сообщения или события, вызвавшего запрос решения. PDP возвращает принятое решение и PEP исполняет его, воспринимая или отвергая запрос. PDP может также вернуть PEP дополнительную информацию, включающую один или множество элементов политики. Эта информация не обязательно связана с решением контроля доступа. Зачастую это может содержать сообщение об ошибке, передаваемое или пересылаемое сообщение.

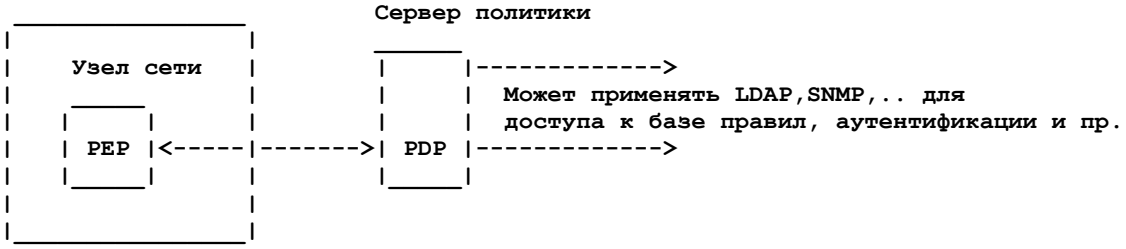

Рисунок 1. Простая конфигурация с основными компонентами архитектуры контроля доступа. PDP может использовать дополнительные механизмы и протоколы для учета, аутентификации, хранения правил и т. п.

PDP может контактировать с другими внешними серверами, например, для доступа к базам данных конфигурации, аутентификации пользователей, учета и оплаты. При таком взаимодействии могут применяться протоколы управления сетями (SNMP) или доступа к каталогам (LDAP). Хотя конкретные типы доступа и протоколы могут различаться в реализациях, некоторые из таких взаимодействий могут иметь влияние на сеть в целом и совместимость устройств.

Особое значение имеет «язык» определения правил, реализованный в PDP. Число правил, применимых к узлу сети, может быть достаточно большим. В то же время эти правила могут быть очень сложными с точки зрения числа полей, используемых для принятия решения, а спектр решений может быть широким. Кроме того, вполне возможно применение нескольких правил к одному профилю запроса. Например, политика может предписывать определенную обработку запросов от общей группы пользователей (например, сотрудники компании), а также иную обработку запросов другой группы (например, управляющих). В этом примере профиль managers соответствует двум правилам, одно из которых является общим, другое - более конкретным.

Чтобы справиться со сложностями принятия решений и обеспечить согласованность политики в рамках сети, язык описания правил должен обеспечивать однозначное сопоставления профиля запроса с действием политики. Язык также должен позволять упорядочение правил или указание приритета для каждого правила. Некоторые из этих вопросов рассмотрены в [6].

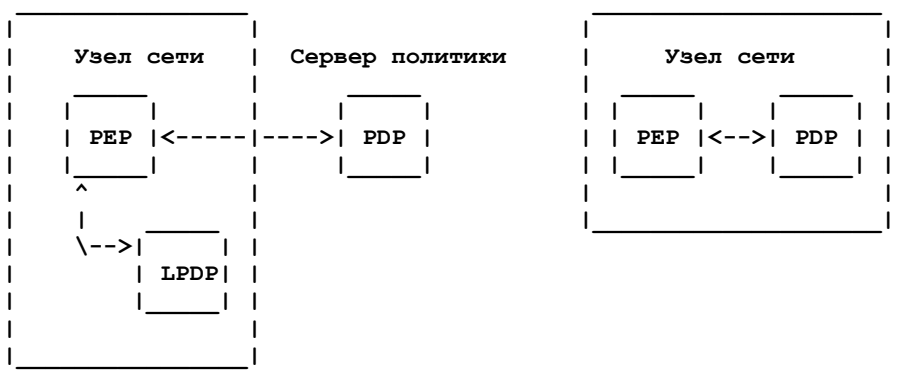

Рисунок 2. Два других варианта конфигурации компонент политки управления доступом. Слева показана локальная точка принятия решений на узле сети, а справа - PEP и PDP на одном узле.

В некоторых случаях простой конфигурации, показанной на рисунке 1, может оказаться недостаточно, поскольку нужно применять локальные правила (например, списки доступа) в дополнение к правилам удаленной точки PDP. Кроме того, PDP может размещаться на одном узле с PEP. Эти варианты показаны на рисунке 2.

Конфигурации, показанные на рисунках 1 и 2, иллюстрируют гибкость разделения задач. С одной стороны, централизованный сервер политики, который может отвечать за принятие решений от имени множества узлов сети в административном домене, может реализовать политику в широкой области (обычно в рамках AD). С другой стороны, правила, зависящие от локальной информации и условий конкретного маршрутизатора, которые более динамичны, эффективней реализовать локально не одном маршрутизаторе.

Когда это доступно, PEP будет сначала использовать LPDP для принятия решения локально. Это частичное решение и исходный запрос затем передаются точке PDP, принимающей окончательное решение (возможно, меняющее решение LPDP). Следует отметить, что PDP представляет окончательное решение, возвращаемое точке PEP, которая должна выполнить решение, принятое PDP. Наконец, если организовано общее состояние для запроса и отклика между PEP и PDP, точка PEP отвечает за информирование PDP о том, что исходный запрос больше не используется.

Если не указано иное, в оставшейся части документа будет применяться конфигурация, показанная слева на рисунке 2.

В этой модели управления политикой модуль PEP на узле сети должен для принятия решения использовать указанные ниже действия.

1. Когда локальное событие или сообщение вызывает PEP для принятия решения, PEP создает запрос, включающий информацию из этого сообщения (или локального состояния), описывающую запрос управления доступом. Кроме того, запрос включает подходящие элементы политики, как указано ниже.
2. PEP может обратиться к локальной базе конфигурации для идентификации набора элементов политики (назовем его A), которые могут быть проверены локально. Локальная конфигурация задает типы элементов политики для локальной оценки. PEP передает запрос с набором A локальной точке принятия решений LPDP и принимает результат LPDP («частичное решение», обозначенное D(A)).
3. Затем PEP передает запрос со **всеми** элементами политики и D(A) точке PDP, которая применяет правила ко всем элементам политики и запроса, принимая решение (обозначено D(Q)). Затем это решение объединяется с частичным решением D(A) для получения окончательного решения.
4. PDP возвращает окончательное решение (полученное при объединении) точке PEP.

Отметим, что в приведенной выше модели точка PEP **должна** контактировать с PDP даже при отсутствии (или NULL) объектов политики, полученных в запросе контроля доступа. Это требование помогает гарантировать для каждого запроса невозможность обойти управление политикой путем пропуска элементов политики в запросе на резервирование. Однако разрешено «короткое замыкание» при обработке, т. е. при отрицательном результате D(A) не требуется выполнять дополнительную проверку в PDP. Тем не менее, нужно информировать PDP об отказе при локальной обработке политики. То же самое относится к случаю, когда обработка политики прошла, но контроль доступа (на уровне управления ресурсом в результате нехватки емкости) дал отрицательный результат. PDP в этом случае также нужно информировать об отказе.

Нужно также отметить, что PDP может в любой момент передать асинхронное уведомление PEP об изменении первоначального решения или сгенерировать сообщение об ошибке политики или предупреждение.

4.1. Пример маршрутизатора RSVP

Для маршрутизатора RSVP на рисунке 3 показано взаимодействие между PEP и другими компонентами int-serv в маршрутизаторе. Для обсуждения все компоненты, относящиеся к связанной с RSVP обработке, показаны в виде одного модуля RSVP, а более подробное обсуждение взаимодействия и интерфейсов между RSVP и PEP дано в [3].

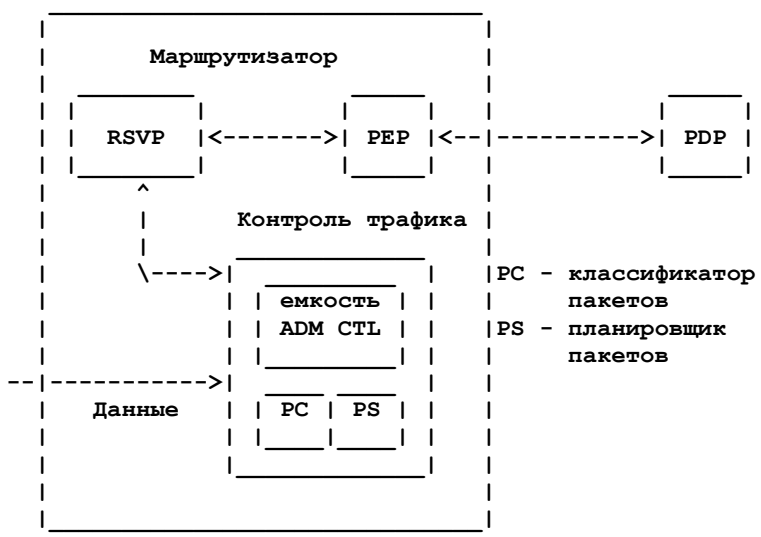

Рисунок 3. Связь между PEP и другими компонентами int-serv в маршрутизаторе RSVP

Когда сообщение RSVP приходит маршрутизатору (или связанное с RSVP событие требует решения политики), предполагается, что модуль RSVP передаст запрос (соответствующий событию или сообщению) модулю PEP, который будет использовать PDP (и LPDP) для принятия решения и возврата его модулю RSVP.

4.2. Дополнительная функциональность PDP

Обычно PDP возвращает окончательное решение на основе запроса управления доступом и связанных элементов политики. Однако у PDP должна быть возможность запросить PEP (или модуль контроля доступа в элементе сети, где размещается PEP) генерацию связанных с политикой сообщений об ошибках. Например, в случае RSVP точка PDP может воспринять запрос и разрешить организацию и пересылку резервирования предыдущему интервалу (hop), но в то же время сгенерировать сообщение об ошибке (предупреждение) нисходящему узлу (NHOP) для информирования о том, что «запрос может быть отменен по истечении 10 минут и т. п.». По сути нужна возможность создавать связанные с политикой сообщения об ошибках и/или предупреждения и распространять их с использованием естественного протокола сигнализации QoS (такого как RSVP). Такие ошибки, возвращаемые PDP, должны также обеспечивать возможность указать, следует ли по-прежнему воспринимать, устанавливать и пересылать запросы резервирования для продолжения обычной обработки RSVP. В частности, возвращенная PDP ошибка указывает, что

1. сообщение, создавшее запрос контроля доступа, следует обработать как обычно, а сообщение об ошибке (или предупреждение) следует передать в другом направлении и включить в него объекты политики, указанные в сообщении об ошибке;
2. или указывает, что была возвращена ошибка, но сообщение RSVP не следует пересылать как обычно.

4.3. Взаимодействие PEP, LPDP и PDP на маршрутизаторе RSVP

Все детали обработки сообщений RSVP и связанных с ними взаимодействий между разными элементами в маршрутизаторе RSVP (PEP, LPDP) и PDP описаны в отдельных документах [3,8]. Ниже приведены несколько аспектов, связанных с рассматриваемой моделью.

- Точка LPDP является необязательной и может применяться для принятия решений на основе локально обрабатываемых элементов политики. LPDP для принятия решений могут потребоваться внешние объекты (такие, как служба каталогов, сервер аутентификации и т. п.).
- PDP поддерживает состояние и может принимать решения даже при отсутствии полученных объектов политики (т. е. принимать решение на основе такой информации как спецификация потока и объект сессии в сообщениях RSVP). PDP может обращаться к другим PDP, но коммуникации и координация между PDP выходят за рамки этого документа.
- PDP передает асинхронные уведомления PEP, когда нужно изменить предшествующие рещения, сообщить об ошибке и т. п.
- PDP экспортирует информацию, полезную для мониторинга и учета использования. Примером полезного механизма может служить MIB или реляционная база данных. Однако этот документ не задает какого-либо конкретного механизма и рассмотрение таких механизмов выходит за рамки документа.

4.4. Размещение элементов политики в сети

Обеспечивая разделение задач между LPDP и PDP, архитектура управления политикой позволяет поэтапное развертывание путем включения маршрутизаторов различной степени сложности в части управления политикой взаимодействовать с серверами политики. На рисунке 4 приведен пример набора узлов в трех административных доменах (AD), каждый из которых относится к своему сервис-провайдеру. Узлы A, B, C относятся к AD-1, обслуживаемому PDP PS-1, а D и E относятся к AD-2 и AD-3, соответственно. Узел E взаимодействует с PDP PS-2. В общем случае предполагается наличие хотя бы одной точки PDP в каждом административном домене.

Узлы сети с поддержкой политики могут быть простыми как E, у которых нет LPDP и они вынуждены опираться на внешнюю точку PDP для каждой обработки правил или самодостаточными как D, который имеет локальные LPDP и PDP в составе маршрутизатора.

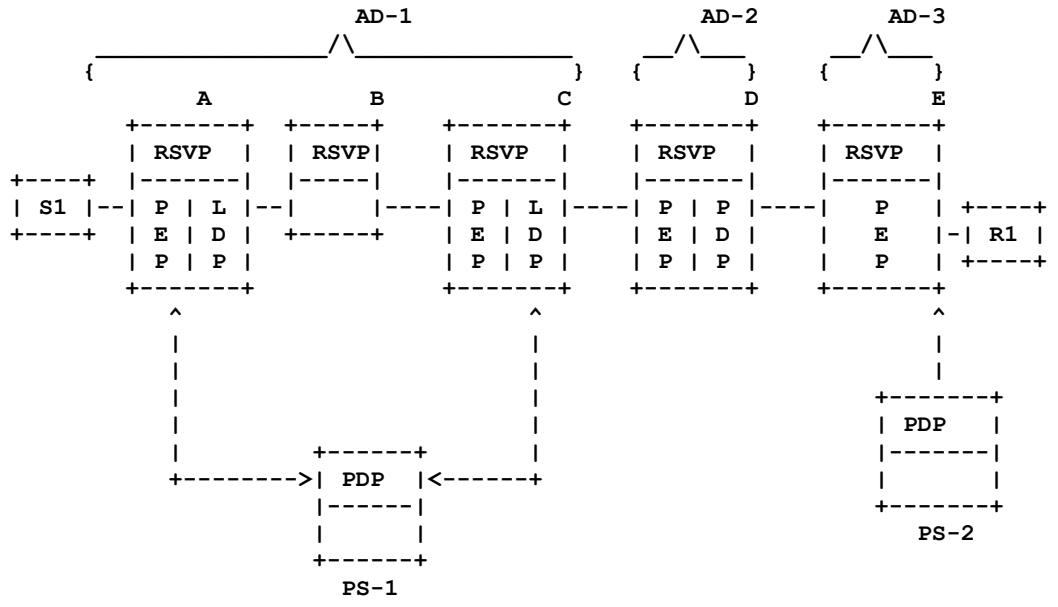

Рисунок 4. Размещение элементов политики в сети.

5. Примеры политики, сценариев и поддержки политики

Далее представлены примеры политики и сценариев, требующих управления политикой, которые должна поддерживать модель управления политикой. В некоторых случаях изложены возможные подходы к достижению желаемых целей с перечнем нерешенных вопросов.

5.1. Правила восприятия на основе времени, отождествления и свидетельств

Контроль политики должен позволять выразить и выполнить правила с временными зависимостями. Например, группе пользователей может быть разрешено резервирование ресурсов на неком уровне лишь в часы отсутствия пиковой нагрузки. Кроме того, контроль политики должен поддерживать правила, учитывающие отождествление или свидетельство пользователя, запрашивающего определенную услугу или ресурс. Например, запрос на резервирование RSVP может быть принят или отвергнут в зависимости от представленного пользователем отождествления или свидетельства.

5.2. Двухсторонние соглашения между сервис-провайдерами

До недавнего времени соглашения между сервис-провайдерами для трафика через границу доменов были достаточно простыми. Наример, два ISP могли согласовать восприятие любого трафика друг от друга без учета и оплаты пропускания «чужого» трафика. Однако доступность механизмов QoS, основанных на интеграции и дифференциации услуг, дифференциация трафика и гарантий качества обслуживания, привела к их постепенному внедрению в Internet. По мере того, как ISP начинают продавать своим пользователям различные уровни обслуживания и могут различать разные виды трафика, они будут искать механизмы оплаты друг другу трафика (и резервирования) через свои сети. Еще одним стимулом для создания таких механизмов является асимметрия трафика в терминах клиентской базы разных провайдеров. ISP, ориентированные на корпоративных заказчиков, скорей всего будут иметь более высокий спрос на резервирование по сравнению с провайдерами, обслуживающими индивидуальных пользователей. Отсутствие изощренных схем учета трафика между ISP может привести к неэффективному распределению затрат между разными сервис-провайдерами.

Двухсторонние соглашения можно разделить на две большие категории — локальные и глобальные. Сложность проблемы вынуждает предположить, что сначала будут применяться лишь первые. В них провайдеры, управляющие сетевым облаком или административным доменом, будут заключать договор со своим ближайшим соседом для задания основных правил и механизмов контроля доступа и учета. Эти договоры будут в основном локальными и не будут опираться на глобальные соглашения, поэтому узлы политики будут поддерживать лишь информацию о соседях. Применительно к рисунку 4, это подразумевает, что провайдер AD-1 будет иметь соглашение об использовании сети с AD-2, но не с AD-3. Провайдер AD-2 будет иметь соглашение с AD-3 и т. д. Таким образом, при пересылке запроса на резервирование в AD-2 провайдер AD-2 будет взимать плату с AD-1 за использование ресурсов вне сети AD-1. Эта информация получается путем рекурсивного применения двухсторонних соглашений на каждой границе между доменами (соседями), пока не дойдет до конечного получателя резервирования. Для реализации такой схемы в архитектуре управления политикой граничные узлы должны добавлять соответствующий объект политики в сообщение RSVP перед его пересылкой в сеть соседнего провайдера. Этот объект будет включать информацию о создавшем его провайдере и эквивалент учетного номера, по которому будут собираться данные для оплаты услуг. Поскольку соглашения существуют лишь между соседями, объекты политики должны заменяться в сообщениях RSVP при пересечении границы административного домена или сети провайдера.

5.3. Правила контроля доступа на основе приоритета

Во многих случаях полезно различать резервирование на основе того или иного уровня «важности». Например, это может оказаться полезным для предотвращения ситуаций, когда первое предоставленное резервирование сможет использовать выделенные ресурсы неограниченно долго. Также это может быть полезно для организации экстренных вызовов в периоды высокой загрузки. Такая функциональность может поддерживаться путем связывания приоритета с запросами резервирования и передачи этой информации вместе с другими данными политики.

В базовом варианте связанный с резервированием приоритет непосредственно определяет право на резервирование запрошенных ресурсов. Если приоритет задается целым числом от 0 до 32 и значение 32 указывает высший приоритет, резервирование с приоритетом, например, 10 будет восприниматься сразу же, если ресурсов, не занятых запросами с более низким приоритетом, достаточно для выполнения этого запроса. Если же таких ресурсов (пропускной способности, буферов и т. п.) недостаточно для выполнения запроса с приоритетом 10, узел будет пытаться освободить ресурсы, путем вытеснения резервов с более низким уровнем приоритета.

Имеется ряд требований, связанных с поддержкой приоритетов и корректным использованием их. Во-первых, система управления трафиком в маршрутизаторе должна знать о приоритетах, т. е. классифицировать имеющиеся резервирования по их приоритетам, чтобы можно было определить, какие резервы и в каком объеме следует вытеснять для выполнения запросов с более высоким приоритетом. Во-вторых, важна согласованность вытеснения на разных узлах для предотвращения переходной нестабильности. В-третьих (возможно, важнее всего), нужно тщательно проектировать слияние приоритетов и понимать его влияние на соответствующие определения политики.

Из трех означенных выше требований слияние данных о приоритете является наиболее сложной задачей и заслуживает дополнительного обсуждения. Сложность слияния данных о приоритете обусловлена тем, что это объединение выполняется в дополнение к слиянию информации о резервировании. Когда данные о резервировании (FLOWSPEC) идентичны (резервирование однородно), при слиянии достаточно рассмотреть информацию о приоритете и простое правило сохранения высшего приоритета дает адекватный ответ. Однако при неоднородном резервировании, «двумерная природа» пар (FLOWSPEC, priority) усложняет их упорядочение и слияние. Описание обработки различных объектов RSVP с приоритетами представлено в работе [7].

5.4. Карты предоплаты и маркеры

В телефонных сетях набирает популярность модель на основе карт с предоплатой. Эта концепция применима и в Internet — пользователи покупают «маркеры», которые могут применяться для доступа к сетевым услугам. Когда пользователь запрашивает резервирование, передавая, например, сообщение RSVP RESV, он представляет уникальный идентификационных маркер, встроенный в объект политики. Обработка такого маркера на поддерживающем политику маршрутизаторе приводит к снижению числа «единиц обслуживания» для этого маркера.

Возвращаясь к рисунку 4, предположим, что получатель R1 в административном домене AD3 хочет зарезервировать услугу из AD1. R1 генерирует объект данных политики типа PD(prc, CID), где prc означает карту предоплаты, а CID указывает номер карты. Вместе с другими объектами политики в сообщении RESV этот объект приходит на узел E, который пересылает его своей точке PEP (PEP_E), а так обращается к PDP PS-3. Точка PS-3 обращается к локальной

или удаленной карт предоплаты. Если кредит карты с номером CID не исчерпан, PDP разрешает резервирование и объект политики возвращается PEP_E. Здесь нужно решить два вопроса:

- какова область действия оплаты?
- когда оплата происходит в первый раз (в форме снижения остатка)?

Ответ на первый вопрос связан с действующими двухсторонними соглашениями. Если провайдер AD-3 имеет соглашения с AD-2 и AD-1, он будет оплачивать стоимость полного резервирования вплоть до отправителя S1. В этом случае PS-2 удалит объект PD(prc,CID) из отправляемого сообщения RESV.

Если же у AD-3 нет двухсторонних соглашений, он просто будет снимать с CID плату за резервирование внутри AD-3 и пересылать PD(prc,CID) в исходящем сообщении RESV. Следующие PDP в других административных доменах также снимут с CID плату за свое резервирование. Поскольку множество объектов считывает (оставшиеся средства) и записывает (снятие оплаты) информацию в одну базу данных, требуется тот или иной контроль доступа к базе и блокировка записи. Вопросы, связанные с размещением, поддержкой и координацией платежных баз данных выходят за рамки этого документа.

Другая проблема связана с фиксацией исчерпания средств (кредита). Точкам PDP следует периодически обращаться к базе данных для списания средств с карты CID. Если оплаченные средства закончились, потребуется механизм отзыва или прерывания обслуживания на основе этой карты.

Что касается момента начала взимания платы, в идеале это должно происходить после успешного выполнения запроса на резервирование. При локальной оплате эта информация может передаваться маршрутизатором точке PDP.

5.5. Заданные отправителем ограничения на резервирование

Возможность задания отправителем ограничений на резервирование с учетом отождествления получателя, числа получателей или стоимости резервирования может быть полезна в будущих сетевых приложениях. Примером может служит любое приложение, в котором отправитель платит за предоставление услуги получателям. В таких случаях отправитель может быть готов взять на себя оплату резервирования при выполнении некоторых условий, например, наличия получателя в списке доступа (ACL[1]) и соответствия некому пределу расходов (отметим, что это позволяет создавать «закрытые» multicast-группы).

В политике, основанной на модели контроля доступа, такая схема может быть реализована путем генерации отправителем соответствующих объектов политики, передаваемых в сообщениях PATH, которые организуют состояния на маршрутизаторах по пути к получателю. Принимая резервирование маршрутизаторы будут сравнивать запросы RESV с установленным состоянием.

Для этого варианта может быть множество решений, точное описание которых выходит за рамки документа.

6. Взаимодействие между PEP и PDP

В случае внешнего PDP нужен протокол для коммуникаций между PEP и PDP. Для обеспечения взаимодействия между сетевыми элементами разных производителей и (внешними) серверами политики этот протокол должен быть стандартизованным.

6.1. Требования к протоколу между PEP и PDP

В этом разделе приведены общие требования к протоколу взаимодействия между PEP и внешней точкой PDP.

Надежность

Важность данных управления политикой требует надежной работы. Незамеченная потеря запросов или откликов может приводить к несогласованности операций управления сетью и явно неприемлема для таких операций, как учет и выставление счетов. Одним из вариантов обеспечения надежности служит использование транспорта TCP.

Малые задержки

Временные рамки принятия решений, связанных с сигнальными протоколами QoS, предполагаются достаточно жесткими. Протокол взаимодействия между PEP и PDP должен обеспечивать минимальную задержку откликов на запросы PEP к PDP.

Способность передавать неразобранные объекты

Протокол должен обеспечивать доставку самоопределяемых, не анализируемых объектов переменного размера, таких как сообщения и объекты политики RSVP и другие объекты, которые могут быть определены при введении новой политики. Протокол не должен требовать изменений при добавлении новых объектов обмена.

Поддержка инициируемых PEP двухсторонних транзакций

Протокол должен разрешать двухсторонние транзакции (запрос-отклик) между PEP и PDP. В частности, для PEP должна обеспечиваться возможность инициировать запрос решения, повторное согласование принятого ранее решения и обмен данными политики. В некоторой степени это требование тесно связано с целью относящегося к RSVP контроля доступа на основе правил. Сигнальные события RSVP, такие как получение сообщений RESV, тайм-аут состояния или слияние резервирования требуют от PEP (таких как маршрутизаторы RSVP) запрашивать решение у PDP в любой момент. Кроме того, у PEP должна быть возможность сообщать данные мониторинга и изменения состояний точкам PDP в любой момент.

Поддержка асинхронных уведомлений

Это нужно для того, чтобы сервер политики и клиент могли уведомлять друг друга при асинхронных (не вызванных сигнальным сообщением) сменах состояния. Например, сервер должен сообщать клиенту об отмене имеющегося резервирования по истечении пользовательских свидетельств или исчерпании баланса счета. Клиент должен информировать сервер об отвергнутом в результате контроля доступа резервировании.

Обслуживание multicast-групп

Протоколу следует обеспечивать обработку решений, относящихся к multicast-группам.

Спецификация QoS

Протоколу следует разрешать точное задание уровня требований к сервису. В запросах PEP, пересылаемых PDP.

[1]Access control list — список управления доступом.

7. Вопросы безопасности

Коммуникационный туннель между сервером и клиентом политики следует защищать с помощью IPSEC [4]. рекомендуется применять для таких туннелей оба протокола AH[1] и ESP[2], чтобы обеспечить конфиденциальность, целостность, аутентификацию источника данных и защиту от повторного использования пакетов.

В случае сигнализации RSVP может применяться аутентификация сообщений RSVP MD5 [2] для защиты коммуникаций между элементами сети.

8. Литература

[1] Braden, R., Zhang, L., Berson, S., Herzog, S. and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

[2] Baker, F., Lindell, B. and M. Talwar, "RSVP Cryptographic Authentication", RFC 2747, January 2000.

[3] Herzog, S., "RSVP Extensions for Policy Control", RFC 2750, January 2000.

[4] Atkinson, R., "Security Architecture for the Internet Protocol", RFC 1825[3], August 1995.

[5] Rigney, C., Rubens, A., Simpson, W. and S. Willens, "Remote Authentication Dial In User Service (RADIUS)", RFC 2138[4], April 1997.

[6] Rajan, R., et al., "Schema for Differentiated Services and Integrated Services in Networks", Work in Progress.

[7] Herzog, S., "RSVP Preemption Priority Policy", Work in Progress.

[8] Herzog, S., "COPS Usage for RSVP", RFC 2749, January 2000.

9. Благодарности

Эта работа является результатом обсуждений среди членов группы RAP, включая Jim Boyle, Ron Cohen, Laura Cunningham, Dave Durham, Shai Herzog, Tim O'Malley, Raju Rajan и Arun Sastry.

10. Адреса авторов

Raj Yavatkar

Intel Corporation

2111 N.E. 25th Avenue,

Hillsboro, OR 97124

USA

Phone: +1 503-264-9077

EMail: raj.yavatkar@intel.com

Dimitrios Pendarakis

IBM T.J. Watson Research Center

P.O. Box 704

Yorktown Heights

NY 10598

Phone: +1 914-784-7536

EMail: dimitris@watson.ibm.com

Roch Guerin

University of Pennsylvania

Dept. of Electrical Engineering

200 South 33rd Street

Philadelphia, PA 19104

Phone: +1 215 898-9351

EMail: guerin@ee.upenn.edu

Перевод на русский язык

Николай Малых

[1]Authentication Header — заголовок аутентификации.
[2]Encapsulating Security Payload — инкапсуляция защищенных данных.
[3]Заменен RFC 2401. *Прим. перев.*
[4]Заменен RFC 2865. *Прим. перев.*

nmalykh@protocols.ru

11. Полное заявление авторских прав

Подтверждение

Финансирование функций RFC Editor обеспечено Internet Society.