УДК 004.052

А.Ю. Исхаков, С.Ю. Исхаков, О.А. Кондратова, Н.Т. Югов

Обеспечение безопасности оборудования Cisco Systems с помощью списков контроля доступа

Рассматривается технология списков контроля доступа (СКД) как средство обеспечения безопасности сетевого оборудования Cisco Systems. Предлагается способ определения типа списков контроля доступа в зависимости от требований сети, отмечаются достоинства и недостатки каждого типа, приводятся возможные способы устранения неполадок, возникающих при использовании данной технологии.

Ключевые слова: безопасность, локально-вычислительная сеть (ЛВС), списки контроля доступа.

Общие сведения о списках контроля доступа

Процесс администрирования вычислительной сети неизбежно связан с необходимостью обеспечения контроля доступа к её ресурсам. С увеличением числа подключений маршрутизатора к внешним сетям администраторы должны решить сложную задачу по обеспечению разделения уровней доступа к данным и настройке качества обслуживания (QoS) [4]. В сетях, построенных на оборудовании Cisco Systems, одним из способов решения данной задачи является использование СКД, предлагающих важные функции безопасности и позволяющие фильтровать пакеты на интерфейсах маршрутизатора. Кроме того, часто данный инструментарий используется для классификации и разделения трафика. Классификация позволяет применять особую обработку к трафику, заданному в СКД, в частности: определять тип трафика для шифрования через VPN-подключение [1]; определять маршруты, которые должны быть перераспределены из одного протокола маршрутизации в другой; использовать фильтрацию в обновлениях маршрутизации и т.д.

В операционной системе Cisco IOS [1] СКД могут контролировать транзитные потоки трафика, проходящего через все интерфейсы маршрутизатора. Существует возможность конфигурации для входящего и исходящего трафика Telnet [4] на портах VTY [1] для администрирования маршрутизатора.

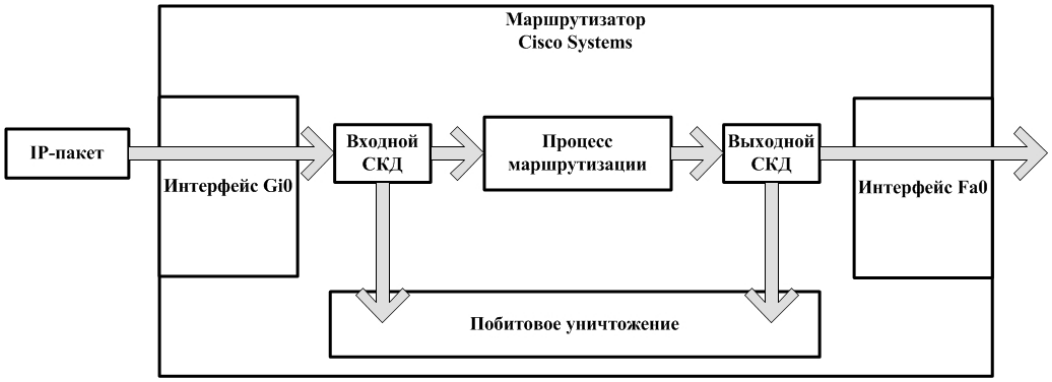

Рис. 1. Принципиальная схема работы СКД

СКД представляют набор правил, регламентирующих процедуру обработки пакетов. Данные правила не применяются к пакетам, сгенерированным самим маршрутизатором. СКД могут работать применительно к входящему и исходящему типу трафика.

Инструкции СКД выполняются в логической последовательности. Они оценивают пакеты сверху вниз по одной инструкции за раз. Если заголовок пакета соответствует правилу СКД, остальные инструкции пропускаются. В противном случае пакет проверяется на соответствие следующей записи в списке. Данный процесс повторяется до конца списка инструкций.

Типы списков контроля доступа

1) Стандартные СКД. Проверяют адреса источников маршрутизируемых пакетов по протоколу IP. В результате данные полного пакета протоколов принимаются или отклоняются в зависимости от IP-адреса сети-источника, подсети или хоста [3].

2) Расширенные СКД. Проверяют адреса источника и назначения, протоколы, номера портов и другие параметры, что обеспечивает администраторам дополнительную гибкость в реализации политики безопасности.

3) Дополнительные типы: динамические (ДСКД), рефлексивные (РСКД) и временные (ВСКД). Основываются на первых двух типах и обеспечивают дополнительные функциональные возможности.

Существуют два типа идентификации стандартных и расширенных СКД: использование нумерации или описательного имени. Для каждого протокола можно создать несколько СКД с разными номерами. Для каждого протокола, направления и интерфейса можно задать только один СКД. Номера списков от 1 до 99 и от 1300 до 1999 настраивает маршрутизатор на принятие инструкций стандартного нумерованного СКД для IPv4 [3]. Для расширенного – от 100 до 199 и от 2000 до 2699 соответственно. Последовательная нумерация записей списков доступа по протоколу IP предлагает возможность изменения порядка инструкций и удаления отдельных записей.

ДСКД необходимо использовать, чтобы удалённый пользователь или группа пользователей получили доступ к сети с удалённых хостов через Интернет. ДСКД аутентифицирует пользователей и разрешает ограниченный доступ через брандмауэр-маршрутизатор к хосту или подсети в течение конечного периода времени. Данный инструментарий позволяет разрешить доступ к удалённым ресурсам ограниченному набору локальных хостов. ДСКД требует аутентификации через TACACS+ [5] или другой сеансовый протокол.

РСКД обеспечивают фильтрацию IP-пакетов в соответствии с данными сеанса верхнего уровня. Они используются для разрешения исходящего трафика и ограничения входящего трафика в ответ на сеансы, созданные в сетях маршрутизатора. РСКД генерируют временные записи при запуске нового сеанса IP. Данные списки вносятся в расширенный именованный СКД, который активируется на интерфейсе.

ВСКД поддерживают контроль доступа в зависимости от временной характеристики [6]. Чтобы внедрить ВСКД, необходимо задать диапазон времени для каждого дня и недели. Временной диапазон идентифицируется именем, на которое ссылается функция. Вследствие этого временные ограничения применяются к самой функции [7].

В таблице представлен список выявленных преимуществ СКД 3 по сравнению со стандартными и статистическими расширенными списками.

Преимущества для системы безопасности в случае использования СКД 3-го типа

Тип СКД	Преимущества
ДСКД	Использование механизма вызова для аутентификации отдельных пользователей
	Упрощённое управление в крупных интерсетях
	Снижение объёма вычислений на маршрутизаторе
	Динамический доступ пользователя через брандмауэр, не подвергающий риску другие ограничения безопасности
РСКД	Защита от подделки пакетов и Dos-атак [5]
	Гибкость в контроле пакетов
ВСКД	Дополнительный контроль над доступом пользователей к ресурсам
	Возможность задания политики безопасности в зависимости от времени: 1) Безопасность на основе периметра с использованием функций Cisco IOS Firewall. 2) Конфиденциальность на основе Cisco Encryption Technology или IP Security
	Усовершенствованная функция маршрутизации на основе политик и очередей
	Возможность обеспечения экономичной автоматической маршрутизации трафика

После завершения настройки СКД необходимо воспользоваться командами show для того, чтобы проверить конфигурацию. Команда show-access-lists отображает содержимое всех СКД; поддерживается использование дополнительного параметра номера или имени конкретного списка. Для вывода содержимого СКД по протоколу IP необходимо использовать команду show ip-access-list.

Заключение

Правильное использование и настройка СКД несомненно являются одной из важнейших задач во время конфигурации маршрутизаторов. Стандартные и расширенные СКД операционной системы Cisco IOS используются для классификации IP-пакетов. Данный инструментарий предоставляет возможность использования различных средств безопасности, маршрутизации на основе политик, а

также применения приоритета обслуживания. Эти функции активируются на интерфейсах маршрутизаторов и коммутаторов в определённом направлении (входящем и исходящем).

Работа выполнена в рамках проекта 7.701.2011 (проект 1/12) при поддержке Министерства образования и науки Российской Федерации.

Литература

1. Odom W. CCNA ICND2 Official Exam Certification Guide (CCNA Exams 640-816 and 640-802) – 2011. – Part. 2. – P. 62–66.

2. Исхаков А.Ю. Методы и средства контроля и мониторинга трафика на коммутаторах Cisco Systems // Матер. Всерос. науч.-техн. конф. студентов, аспирантов и молодых ученых «Научная сессия ТУСУР–2012», Томск, 16–18 мая 2012 г. – Томск: В-Спектр, 2011. – Ч. 3. – С. 40–43.

3. Пакетные фильтры и их конфигурирование [Электронный ресурс]. – Режим доступа: http://cisco.far.ru/acl.html, свободный (дата обращения: 10.03.2012).

4. ACL: списки контроля доступа в Cisco IOS [Электронный ресурс]. – Режим доступа: http://habrahabr.ru/post/121806/, свободный (дата обращения: 3.03.2012).

5. Исхаков А.Ю. Обеспечение безопасности системы управления сетью / А.Ю. Исхаков, С.Ю. Исхаков // Сб. тр. VIII Всерос. науч.-практ. конф. студентов, аспирантов и молодых ученых «Технологиии Microsoft в теории и практике программирования», Томск, 23–24 марта 2011 г. – Томск: Изд-во Том. политех. ун-та, 2011. – С. 214–215.

6. Ходашинский И.А. Методы нечеткого извлечения знаний в задачах обнаружения вторжений / И.А. Ходашинский , И.В. Горбунов, Р.В. Мещеряков // Вопросы защиты информации. – 2002. – № 1. – С. 45–50.

7. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Спец. Вып. 1. – С. 51–61.

Исхаков Андрей Юнусович
Инженер каф. КИБЭВС ТУСУРа
Тел.: 8 (382-2) 900-111, доп. 25-16
Эл. почта: iay@security.tomsk.ru

Исхаков Сергей Юнусович:
Аспирант каф. КИБЭВС ТУСУР
Тел. : 8 (382-2) 41-34-26
Эл. почта: iskhakovsy@oez.tomsk.ru

Кондратова Ольга Анатольевна
Канд. техн. наук, проф. каф. ЕНПД Новокузнецкого филиала
Национального исследовательского Томского политехнического университета
Тел.: 8-923-532-23-70
Эл. почта: okondratova@mail.ru

Югов Николай Тихонович
Д-р физ.-мат. наук, проф. каф. высшей математики ТУСУРа
Тел.: 8 (382-2) 41-34-26
Эл. почта: office@keva.tusur.ru

Iskhakov A.Y., Iskhakov S.Y., Kondratova O.A., Ugov N.T.
Securing Cisco Systems equipment with access control lists

The technology of access control lists (ACL) as a means of ensuring security of network equipment Cisco Systems are described.
Keywords: Cisco Systems, local area network, access control lists.