Владимиров С.Н., Карельская К.А., Михальцов Н.Г. Выбор протокола для реализации централизованного управления пользователями на различном оборудовании и сервисах. // Проблемы информатики в образовании, управлении, экономике и технике: Сб. статей XVIII Междунар. научно-техн. конф. – Пенза: ПДЗ, 2018. – С. 110-113.

УДК 004.822

ВЫБОР ПРОТОКОЛА ДЛЯ РЕАЛИЗАЦИИ ЦЕНТРАЛИЗОВАННОГО УПРАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМИ НА РАЗЛИЧНОМ ОБОРУДОВАНИИ И СЕРВИСАХ

С.Н. Владимиров, К.А. Карельская, Н.Г. Михальцов

CHOICE OF A PROTOCOL FOR IMPLEMENTATION OF A CENTRALIZED USER MANAGEMENT ON VARIOUS EQUIPMENT AND SERVICES

S.N. Vladimirov, K.A. Karelskaya, N.G. Mikhaltsov

Аннотация. В статье рассматриваются протоколы для реализации аутентификации, авторизации и сбора сведений об использованных ресурсах, разработанные для передачи данных между центральной платформой и оборудованием.

Ключевые слова: AAA-сервер, аутентификация, авторизация, учет.

Abstract. The article discusses protocols for obtaining authentication, authorization, and gathering information about the resources used, designed to transfer information between the corporation and the equipment.

Keywords: AAA-server, authentication, authorization.

В крупных организациях при использовании большого количества устройств и сервисов, на которых надо проходить аутентификацию, необходима учетная запись для каждого пользователя. При изменении данных пользователя, удалении пользователя или добавлении нового необходимо проводить манипуляции с его учетной записью на каждом устройстве или сервисе. При их большом количестве это является трудоемкой задачей. Для решения этой задачи существует AAA-механизм.

На данный момент существуют три протокола, относящихся к AAA (Authentication, Authorization, Accounting): Remote Authentication Dial-In User Service (RADIUS), Cisco’s Terminal Access Controller Access-Control System Plus (TACACS+) протоколы и DIAMETER.

Аутентификация (authentication) – идентификация пользователя, как правило, путем ввода пользователем правильного имени пользователя и действительного пароля до получения доступа. Процесс аутентификации основан на каждом пользователе, имеющем уникальный набор критериев для получения доступа. Сервер AAA сравнивает учетные данные пользователя с другими учетными данными пользователя, хранящимися в базеданных. Если учетные данные совпадают, пользователю предоставляетсядоступ к сети. Если учетные данные отклоняются, аутентификация завершается сошибкой, а доступ к сети запрещен.

Авторизация (authorization) – следующий шаг после успешной аутентификации. Процесс авторизации определяет, имеет ли пользователь право выдавать такие команды. Проще говоря, авторизация – это процесс обеспечения соблюдения политик: определение типов или свойств видов деятельности, ресурсов или услуг, которым разрешен пользователь. Обычно авторизация происходит в контексте аутентификации. После аутентификации пользователя они могут быть авторизованы для разных типов доступа или деятельности.

Учет (accounting) – параллельный с аутентификацией и авторизацией этап, который записывает в журнал успех или неудачу данных процессов, смог человек проникнуть в помещение или нет, получил ли пользователь доступ к сетевому устройству и если да, то какие действия на нем совершал. Этот процесс важен с точки зрения безопасности и контроля доступа, так как позволяет определять потенциальные угрозы и искать «дыры» в системе.

Поскольку при централизации управления пользователей существует несколько решений, необходимо выбрать подходящий вариант. Были рассмотрены протоколы AAA, такие как TACACS+ (Terminal Access Controller Access Control System), RADIUS (Remote Authentication in Dial-In User Service), DIAMETER. В таблице представлено сравнение основных параметров AAA-протоколов. Из таблицы видно, что протоколы TACACS+ и DIAMETER шифруют передаваемые пакеты целиком, а RADIUS только пароль, оставляя, например, логин пользователя в открытом виде. Это может позволить узнать логин при перехвате сообщения между сервером и клиентом. Это является большим минусом протокола RADIUS. Но при этом протокол TACACS+ можно использовать только на оборудовании CISCO. Поэтому при всех плюсах данного протокола он подходит только при условии использования только в сетях на основе оборудования CISCO.

Основные параметры AAA-протоколов

Особенности протоколов	RADIUS	TACACS+	DIAMETER
Базовый протокол	UDP	TCP	TCP
Безопасность	Шифруется только пароль	Шифруется пакет целиком	Шифруется пакет целиком
Возможность перенаправления запросов	Есть	Нет	Есть
Поддержка оборудованием и ПО	Все современное оборудование и ПО	CISCO	Дорогостоящее мощное оборудование

У всех протоколов есть достоинства и недостатки, например TACACS+ использует TransmissionControlProtocol (TCP) порт 49, а не UDP, так как он обладает большей надежностью и позволяет заранее получать информацию о потенциальных ошибках благодаря пакету TCP-

RST. TCP более медленный протокол, но обладает дополнительными преимуществами: возможность разделения аутентификации, авторизации и учета в качестве отдельных и независимых функций, множественная авторизация после одной аутентификации, шифрование всего содержимого пакета. Но при этом он является разработкой компании CISCO, поэтому нет возможности использовать его с устройствами других фирм, производящих сетевое оборудование. Это привязывает пользователя к конкретной фирме и не дает свободы выбора при проектировании информационных систем, в отличие от открытых протоколов RADIUS и DIAMETER. Какой протокол для AAA-сервера использовать, необходимо выбирать в зависимости от задачи. Если это администрирование устройств, то TACACS+ станет лучшим вариантом, а если доступ к сети, то более универсальный и быстрый – RADIUS или DIAMETER. Для реализации централизованного доступа к устройствам и ресурсам сети, основанной на оборудовании разных производителей, необходимо использование AAA-сервера на основе протоколов RADIUS или DIAMETER. Первый протокол поддерживается подавляющим числом устройств и оборудованием, в отличие от протокола DIAMETER.

Поскольку для нашей задачи необходимо использование оборудования без привязки к конкретному производителю, то протокол TACACS+ не подходит. Протокол DIAMETER не удовлетворяет требованиям к оборудованию. Он распространен среди оборудования для сетей большого размера. В нашем случае мы рассматриваем локальную сеть, для которой приобретение такого оборудования нецелесообразно, а также протокол DIAMETER не поддерживается программными продуктами.

Библиографический список

1. Гольдштейн Б.С., Елагин В.С., Сенченко Ю.Л. Протоколы AAA: RADIUS и Diameter. Серия «Телекоммуникационные протоколы». Книга 9 СПб.: БХВ&Петербург, 2014. 352 с.: ил.

2. Описание технологии аутентификации TACACS+, CiscoSystemInc. 2003. URL: http://www.cisco.com/russian_win/warp/public/3/ru/solutions/sec/mer_tech_ident-tacacs.html.

Владимиров Сергей Николаевич
Тверской государственный технический университет,
г. Тверь, Россия
E-mail: slidium1991@yandex.ru

Vladimirov S.N.
Tver State Technical University,
Tver, Russia

Карельская Катерина Александровна
Тверской государственный технический университет,
г. Тверь, Россия
E-mail: kak69@yandex.ru

Karelskaya K.A.
Tver State Technical University,
Tver, Russia

Михальцов Николай Григорьевич
Военная академия
воздушно-космической
обороны имени Маршала
Советского Союза Г.К. Жукова,
г. Тверь, Россия

Mikhaltsov N.G.
Military Academy
of Aerospace defense of Marshall
of the Soviet Union G.K. Zhukov,
Tver, Russia