Сравнение TACACS+ и RADIUS

Содержание

Введение

Двумя наиболее популярными протоколами безопасности, используемыми для управления доступом к сетям, являются TACACS+ и RADIUS корпорации Cisco. Спецификация RADIUS описана в RFC 2865, который obsoletes RFC 2138. Cisco выполняет обязательство поддерживать оба протокола и делает наилучшие предложения в этом классе. Корпорация Cisco не стремится конкурировать с протоколом RADIUS и оказывать какое-либо влияние на пользователей, побуждая их использовать протокол TACACS+. Следует выбирать решение, которое наилучшим образом соответствует вашим потребностям. В данном документе рассматриваются различия между TACACS+ и RADIUS. Эти сведения помогут вам сделать обоснованный выбор.

Корпорация Cisco поддерживает протокол RADIUS с момента выхода выпуска 11.1 ПО Cisco IOS® в феврале 1996 года. Cisco продолжает расширять RADIUS-клиент новыми функциями и возможностями, поддерживая RADIUS как стандарт.

Cisco серьёзно проанализировала RADIUS как протокол безопасности, прежде чем разрабатывать TACACS+. В протокол TACACS+ были включены многие функции для удовлетворения потребностей растущего рынка решений обеспечения безопасности.

Протокол был разработан для масштабирования сетей по мере их роста и адаптации к новой технологии обеспечения безопасности по мере развития рынка. Архитектура, служащая основой протокола TACACS+, дополняет независимую архитектуру аутентификации, авторизации и учета (AAA).

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Общие сведения о RADIUS

RADIUS — это сервер доступа, который использует протокол AAA (аутентификация, авторизация и учет). Эта система распределенной безопасности защищает удаленный доступ к сетям и сетевым службам от несанкционированного доступа. RADIUS содержит три компонента:

- Протокол с форматом кадра, использующим протокол дейтаграмм пользователя (UDP)/IP.
- Сервер.
- Клиент.

Сервер работает на центральном компьютере, как правило, на стороне пользователя, а клиенты размещаются на серверах удаленного доступа и могут распространяться по сети. Cisco внедрила RADIUS-клиент в выпуск 11.1 ПО Cisco IOS и последующие, а также в прикладное ПО для устройств.

Модель "Клиент/сервер"

Сервер доступа к сети (NAS) функционирует как клиент RADIUS. Клиент должен передавать пользовательские данные назначенным серверам RADIUS, а затем действовать в соответствии с полученным ответом. Серверы RADIUS отвечают за получение запросов пользователей на подключение, проверку подлинности пользователей и предоставление всей информации о конфигурации, необходимой клиенту для предоставления услуги пользователю. Серверы RADIUS могут выступать в роли промежуточных клиентов для других типов серверов аутентификации.

Безопасность сети

Подлинность транзакций между клиентом и сервером RADIUS подтверждается с помощью общего секрета, никогда не пересылаемого по сети. Помимо этого, клиент RADIUS отправляет серверу RADIUS зашифрованный пароль пользователя. Это исключает возможность раскрытия пароля пользователя злоумышленником при слежении за незащищенной сетью.

Гибкие механизмы аутентификации

Сервер RADIUS поддерживает разнообразные методы аутентификации пользователя. Для проверки подлинности имени пользователя и пароля, предоставляемых серверу, могут использоваться протоколы PPP ("точка-точка"), PAP (протокол аутентификации по паролю) или CHAP (протокол аутентификации с предварительным согласованием вызова), вход UNIX и другие механизмы аутентификации.

Доступность серверного обеспечения

Существует достаточное количество коммерческого и свободного серверного обеспечения. Cisco предлагает следующие серверы: Cisco Secure ACS для Windows, Cisco Secure ACS для UNIX и Cisco Access Registrar.

Сравнение TACACS+ и RADIUS

В этих разделах приведено сравнение некоторых возможностей TACACS+ и RADIUS.

UDP и TCP

RADIUS использует UDP, а TACACS+ использует TCP. TCP имеет ряд преимуществ по сравнению с UDP. TCP предлагает передачу на основе соединений, в то время как UDP предлагает наилучший сервис доставки. Для протокола RADIUS требуется настройка дополнительных программируемых переменных, например числа попыток повторной передачи или количества тайм-аутов, что делает его одним из наиболее эффективных транспортных протоколов. Однако протокол RADIUS обладает недостаточной, по сравнению с протоколом TCP, встроенной поддержкой:

- Использование TCP обеспечивает отдельное подтверждение получения запроса в течение (приблизительно) времени прохождения сигнала в прямом и обратном направлениях (RTT) по сети, вне зависимости от степени загруженности и медлительности механизма аутентификации на серверной части (и подтверждения TCP).
- TCP обеспечивает немедленную индикацию поврежденного или неработающего сервера, используя сброшенный (RST) набор данных. Можно определить, когда сервер отказывает и возвращается к службе, если используются долговременные подключения TCP. Протокол UDP не может отличить такие ситуации, как неработающий сервер, медленный сервер и несуществующий сервер.
- Использование сообщений проверки активности TCP позволяет определить отказ сервера, не используя полосу пропускания фактических запросов. Возможно одновременное обслуживание подключений к нескольким серверам, требуется только отправить сообщения серверам, о которых известно, что они активны и работают.
- TCP более масштабируем и адаптирован и к росту, и к перегрузке сетей.

Шифрование пакетов

RADIUS шифрует только пароль в пакете запроса доступа от клиента серверу. Остальная часть пакета не шифруется. Прочие сведения, например имя пользователя, авторизованные службы и учёт могут быть перехвачены третьей стороной.

TACACS+ полностью шифрует тело пакета, но оставляет стандартный заголовок TACACS+. Внутри заголовка существует поле, которое показывает, зашифровано тело пакета или нет. Для целей отладки удобно, чтобы тело пакета было не зашифровано. Однако во время обычной работы тело пакета полностью зашифровано для более надёжной связи.

Аутентификация и авторизация

RADIUS сочетает аутентификацию и авторизацию. Сервер RADIUS отправляет клиенту пакеты разрешения доступа, содержащие сведения авторизации. Это усложняет разграничение понятий аутентификации и авторизации.

TACACS+ использует AAA-архитектуру, которая выделяет авторизацию, аутентификацию и учет. Это позволяет параллельно функционировать различным решениям проверки подлинности, которые все еще используют TACACS+ для авторизации и обработки учетных записей. Например, протокол TACACS+ позволяет использовать проверку подлинности Kerberos, а также авторизацию и учет TACACS+. Сначала сервер NAS проверяет подлинность на сервере Kerberos, затем запрашивает сведения авторизации у сервера TACACS+ без повторной аутентификации. Сервер NAS информирует сервер TACACS+ о том, что он успешно прошел проверку подлинности на сервере Kerberos, а сервер после этого предоставляет сведения авторизации.

Если во время сеанса требуется дополнительная проверка подлинности, то сервер доступа выполняет ее с помощью сервера TACACS+, чтобы определить наличие у пользователя разрешения на использование определенной команды. Это предоставляет больший контроль над командами, которые можно выполнять на сервере доступа, разорвав связь с механизмом аутентификации.

Многопротокольная поддержка

Сервер RADIUS не поддерживает следующие протоколы:

- Протокол удаленного доступа AppleTalk (ARA)
- Протокол NetBIOS управления кадрами протоколов канального уровня
- Асинхронный (системный) служебный интерфейс операционной системы NetWare
- Соединение клавиатуры X. 25

TACACS+ обеспечивает многопротокольную поддержку.

Управление маршрутизатором

При использовании протокола RADIUS пользователь не может определять команды, разрешенные или запрещенные для выполнения на коммутаторе. Поэтому протокол RADIUS не так полезен для управления маршрутизатором или не настолько приспосабливаемый для служб терминалов.

TACACS+ предоставляет два способа управления авторизацией команд маршрутизатора по каждому пользователю или по группам. Первый способ состоит в назначении уровней привилегий командам и проверке маршрутизатором с помощью сервера TACACS+ факта авторизации пользователя на указанном уровне привилегий. Для применения второго способа следует явно указать разрешенные команды на сервере TACACS+ для каждого пользователя или для каждой группы.

Совместимость

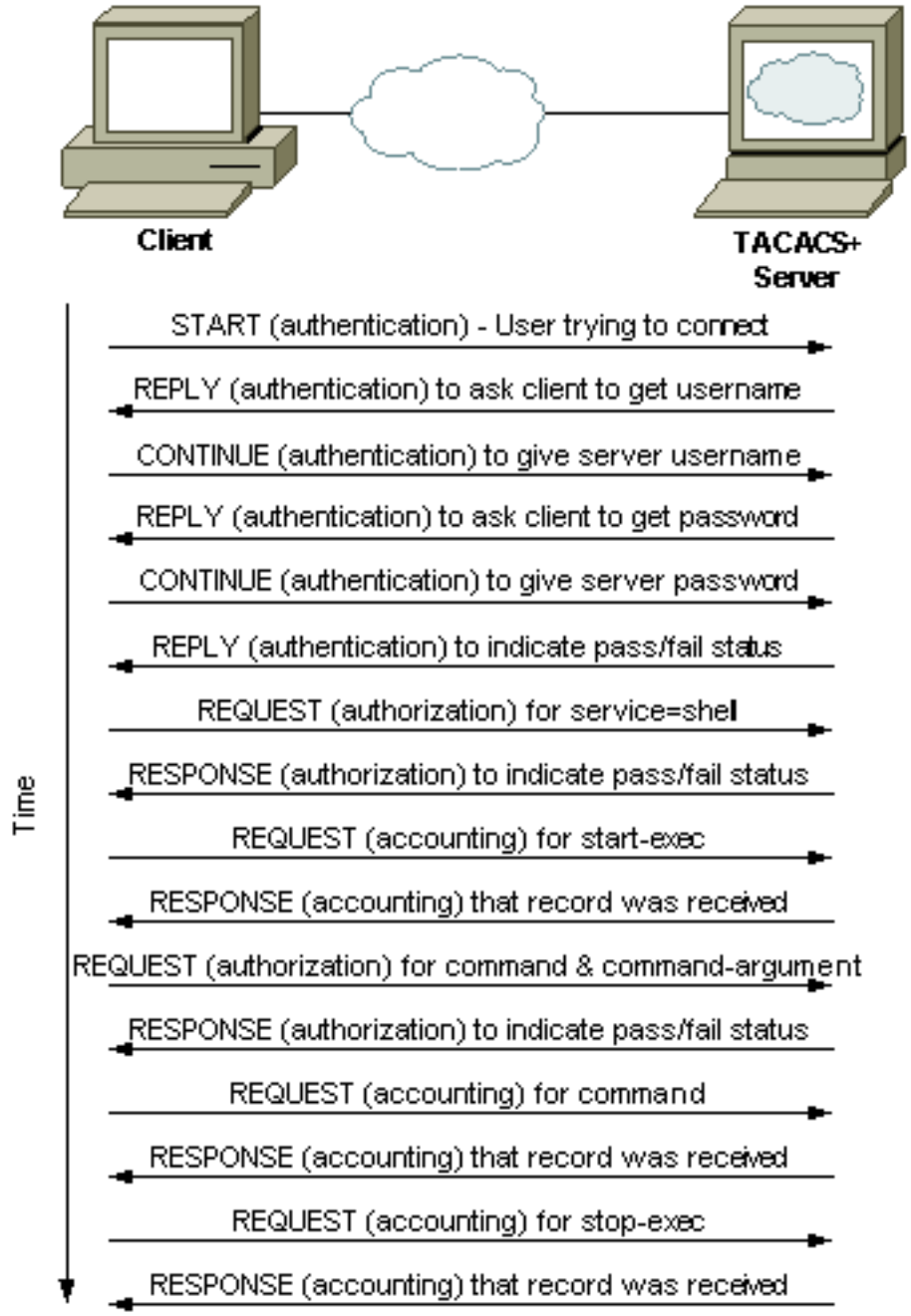
Ввиду различных интерпретаций документов RFC по RADIUS, совместимость с этими документами не гарантирует взаимодействие. Несмотря на то, что несколько поставщиков реализуют клиентов RADIUS, это не означает возможность их взаимодействия. Cisco предоставляет наибольшее число атрибутов RADIUS и последовательно добавляет новые. Если пользователи используют только стандартные атрибуты RADIUS на своих серверах, они могут взаимодействовать между несколькими поставщиками до тех пор, пока эти поставщики предоставляют одинаковые атрибуты. Однако многие поставщики предоставляют расширения, которые являются их собственными атрибутами. Если пользователь использует один из таких специфических расширенных атрибутов поставщика, взаимодействие невозможно.

Трафик

Из описанных выше различий между TACACS+ и RADIUS следует различие объемов трафика, передаваемого между клиентом и сервером. Ниже приведены примеры трафиков между клиентом и сервером для TACACS+ и RADIUS при управлении маршрутизатором с использованием аутентификации, авторизации выполнения, авторизации команд (недоступно для RADIUS), учета выполнения и учета команд (недоступно для RADIUS).

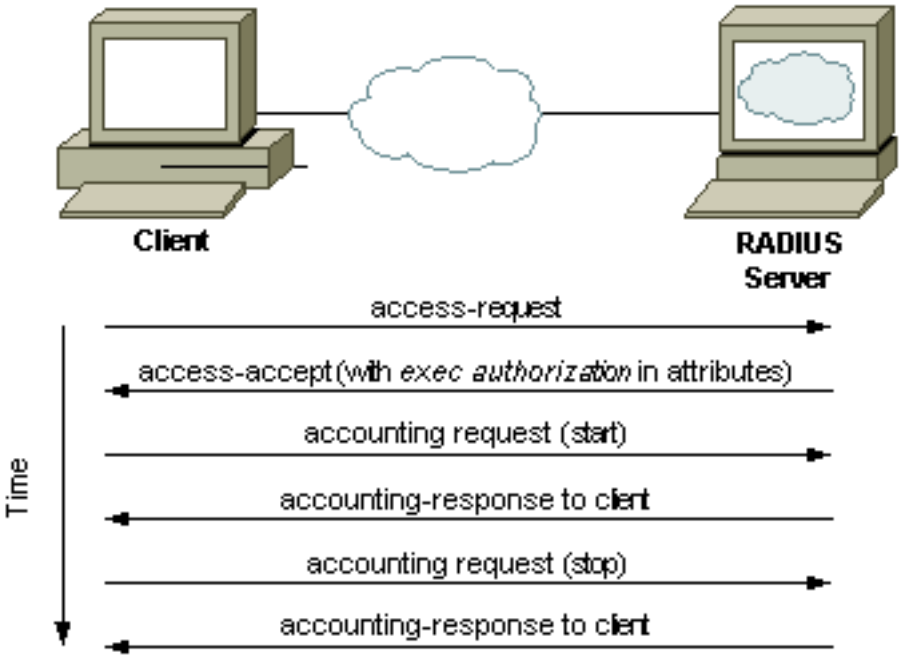
Пример трафика TACACS+

В этом примере предполагается, что с протоколом TACACS+ используется аутентификация имени пользователя, авторизация выполнения, авторизация команд, учет начала и завершения выполнения и учет команд, когда пользователь подключается к маршрутизатору по протоколу Telnet, выполняет команду и отключается:



Пример трафика RADIUS

В этом примере предполагается, что с протоколом RADIUS используется аутентификация имени пользователя, авторизация выполнения и учет начала и завершения выполнения, когда пользователь подключается к маршрутизатору по протоколу Telnet, выполняет команду и отключается (остальные службы управления недоступны):



Поддержка устройств

В данной таблице перечислены AAA TACACS+ и RADIUS, поддерживаемые типом устройства для выбранных платформ. Указана версия программного обеспечения, в которой была добавлена поддержка. Если конкретного продукта нет в этом списке, дополнительную информацию см. в заметках о выпуске продукта.

Устройство Cisco	Аутентификация TACACS+	Авторизация TACACS+	Учет TACACS+	Аутентификация RADIUS	Авторизация RADIUS	Учёт RADIUS
Cisco Aironet1	12.2(4)JA	12.2(4)JA	12.2(4)JA	все точки доступа	все точки доступа	все точки доступа
Программное обеспечение Cisco IOS2	10.33	10.33	10.333	11.1.1	11.1.14	11.1.15
Cisco Cache Engine	--	--	--	1.5	1.56	--
Коммутаторы Cisco Catalyst	2.2	5.4.1	5.4.1	5.1	5.4.14	5.4.15
Коммутатор	5.03	5.03	5.03	5.0	5.04	--

контента Cisco CSS 11000 (Content Services)						
Коммутатор контент-сервисов Cisco CSS 11500	5.20	5.20	5.20	5.20	5.204	--
Межсетевой экран Cisco PIX	4.0	4.07	4.28,5	4.0	5.27	4.28,5
Коммутаторы Cisco Catalyst 1900/2820	8.x корпоративный9	--	--	--	--	--
Коммутаторы Cisco Catalyst 2900XL/3500XL	11.2.(8)SA610	11.2.(8)SA610	11.2.(8)SA610	12.0(5)WC511	12.0(5)WC511,4	12.0(5)WC511,5
Концентратор Cisco VPN 3006	3.0	3.0	--	2.012	2.0	2.012
Концентратор Cisco VPN 5000	--	--	--	5.2X12	5.2X12	5.2X12

Примечания к таблице

1. Завершение сеанса только беспроводных клиентов (без прекращения трафика управления) в версиях ПО Cisco IOS, отличных от версии 12.2(4)JA или более поздних. В ПО Cisco IOS версии 12.2(4)JA и более поздних возможна аутентификация для завершения сеанса беспроводных клиентов и прекращения трафика управления.
2. Информацию о поддержке платформы ПО Cisco IOS проверьте с помощью Feature Navigator (не отменяется Software Advisor (толькозарегистрированные пользователи)).
3. Учёт команд не поддерживается ПО Cisco IOS до выпуска 11.1.6.3.

4. Отсутствует авторизация команд.
5. Отсутствует учёт команд.
6. Блокирование только URL, не административного трафика.
7. Авторизация для не VPN-трафика через PIX.**Примечание:** Версия 5.2 – поддерживается авторизация с использованием атрибута производителя (VSA) списка управления доступом (ACL) RADIUS или авторизация TACACS+ для трафика VPN, оканчивающемся на PIX. Версия 6.1 – поддерживается авторизация с использованием атрибута 11 для ACL RADIUS для трафика VPN, оканчивающегося на PIX. Версия 6.2.2 – поддерживаются загружаемые списки ACL с авторизацией RADIUS для трафика VPN, оканчивающегося на PIX. Версия 6.2 – поддерживается авторизация для управляющего трафика PIX через TACACS+.
8. Учёт только для не VPN-трафика через PIX, без административного трафика.**Примечание:** Версия 5.2 - Поддержка учета пакетов VPN Client TCP через PIX.
9. Только корпоративное ПО.
10. Для образа требуется 8 МБ флэш-памяти.
11. Только оконечные устройства VPN.

Дополнительные сведения

- Страница поддержки RADIUS
- TACACS+ в документации по IOS
- Страница поддержки TACACS/TACACS+
- Запросы комментариев (RFC)
- Cisco Systems – техническая поддержка и документация