Содержание

Введение

Этот документ описывает проблему, с которой встречаются с Ограничением доступа машины (MAR), и предоставляет решение проблемы.

С ростом лично принадлежавших устройств для системных администраторов более важно что когда-либо предоставить способ ограничить доступ к определенным частям сети к корпоративно принадлежавшим активам только. Проблема, описанная в этом документе, касается, как надежно определить эти области интереса и аутентифицировать их без разрушений к возможности подключения пользователя.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с 802.1x, чтобы полностью понять этот документ. Этот документ принимает знакомство с пользовательской аутентификацией 802.1x, и выделяет проблемы и способствует связанный к использованию MAR, и более широко, аутентификация компьютера.

Используемые компоненты

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

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были

запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

MAR в основном пытается решить типичную проблему, свойственную от большинства текущих и популярных методов Протокола EAP, а именно, та аутентификация компьютера и проверка подлинности пользователя являются отдельными, не связанными друг с другом процессами.

Проверка подлинности пользователя является методом аутентификации 802.1x, который знаком большинству системных администраторов. Идея состоит в том, что учетные данные (имя пользователя/пароль) даны каждому пользователю, и что набор учетных данных представляет физическое лицо (это может быть разделено между несколькими людьми также). Поэтому пользователь может войти отовсюду в сети с теми учетными данными.

Аутентификация компьютера является технически тем же, но пользователю, как правило, не предлагают ввести учетные данные (или сертификат); компьютер или машина делают это самостоятельно. Это требует, чтобы машина уже сохранила учетные данные. Передаваемое имя пользователя является **хостом / <MyPCHostname>**, при условии, что ваша машина имеет **<MyPCHostname>** набор как имя хоста. Другими словами, это передает **хост /** придерживавшийся вашим именем хоста.

Несмотря на то, что не непосредственно отнесенный к Microsoft Windows и Active Directory Cisco, этот процесс представлен более легко, если машина соединена с Active Directory, потому что компьютерное имя хоста добавлено к базе данных домена, и об учетных данных выполняют согласование (и возобновляют каждые 30 дней по умолчанию), и сохранил на машине. Это означает, что аутентификация компьютера возможна от любого типа устройства, но это представлено намного более легко и прозрачно если машина соединена с Active Directory, и учетные данные остаются скрытыми от пользователя.

MAR как решение

Легко сказать, что решение для Системы управления доступом (ACS) Cisco или платформы Cisco Identity Services Engine (ISE) для завершения MAR, но существуют преимущества и недостатки для рассмотрения, прежде чем это будет внедрено. Как внедрить, это лучше всего описано в ACS или руководствах пользователя ISE, таким образом, этот документ просто описывает, рассмотреть ли его, и некоторые возможные контрольно-пропускные пункты.

Плюсы

MAR был изобретен, потому что проверки подлинности пользователя и аутентификации компьютера полностью отдельные. Поэтому сервер RADIUS не может принудить проверку, где пользователи должны войти от устройств находившихся в собственности компании. С MAR сервер RADIUS (ACS или ISE, на стороне Cisco) принуждает для данной проверки подлинности пользователя, что должна быть допустимая аутентификация компьютера за эти X часов (как правило, 8 часов, но это конфигурируемо), который предшествует проверке

подлинности пользователя для той же оконечной точки.

Поэтому аутентификация компьютера успешно выполняется, если учетные данные машины известны сервером RADIUS, как правило, если машина соединена с доменом, и сервер RADIUS проверяет это с соединением с доменом. Это полностью до администратора сети, чтобы определить, предоставляет ли успешная аутентификация компьютера полный доступ сети или только ограниченный доступ; как правило, это, по крайней мере, открывает соединение между клиентом и Active Directory так, чтобы клиент мог выполнить такие действия как обновление пароля пользователя или загрузить Объекты Групповой политики (GPOS).

Если проверка подлинности пользователя прибывает из устройства, где аутентификация компьютера не произошла за предыдущие несколько часов, то пользователь запрещен, даже если пользователь обычно допустим.

Полный доступ только предоставляют пользователю, если аутентификация допустима и завершена от оконечной точки, где аутентификация компьютера произошла за несколько прошлых часов.

Недостатки

В этом разделе описываются недостатки использования MAR.

MAR и соискатель Microsoft Windows

Идея позади MAR состоит в том, что для проверки подлинности пользователя, чтобы успешно выполниться, мало того, что у того пользователя должны быть допустимые учетные данные, но и успешная аутентификация компьютера, должен быть зарегистрирован от того клиента также. Если существует какая-либо проблема с этим, пользователь не может аутентифицироваться. Проблема, которая возникает, - то, что эта функция может иногда непреднамеренно локаут легитимный клиент, который вынуждает клиента к перезагрузке для восстановления доступа к сети.

Microsoft Windows выполняет аутентификацию компьютера только во времени загрузки (когда экран входа в систему появляется); как только пользователь вводит учетные данные пользователя, проверка подлинности пользователя выполнена. Кроме того, если выполнены входы пользователя в систему прочь (возвращается к экрану входа в систему), новая аутентификация компьютера.

Вот пример сценария, который показывает, почему MAR иногда вызывает проблемы:

Пользователь X весь день работал на его портативный ПК, который был связан через беспроводное соединение. В конце дня он просто закрывает портативный ПК, и отключения работают. Это размещает портативный ПК в спящий режим. На следующий день он возвращается в офис и открывает свой портативный ПК. Теперь, он неспособен установить беспроводное соединение.

Когда Microsoft Windows в спящем режиме, он берет снимок системы в ее текущем состоянии, которое включает контекст того, в кого вошли. Быстро, кэшированная запись MAR для пользовательского портативного ПК истекает и очищена. Однако, когда

портативный ПК включен, он не выполняет аутентификацию компьютера. Это вместо этого идет прямо в проверку подлинности пользователя, начиная с того, именно это сделал запись спящий режим. Единственный способ решить это состоит в том, чтобы регистрировать пользователя прочь, или перезагружать его компьютер.

Несмотря на то, что MAR является хорошей функцией, он имеет потенциал для порождения разрыва сети. Этих разрушений трудно устранить неполадки, пока вы не понимаете способ, которым работает MAR; при реализации MAR важно рассказать конечным пользователям о том, как должным образом завершить работу компьютеров, и выйдите из системы каждой машины в конце каждого дня.

MAR и различные серверы RADIUS

Распространено иметь несколько серверов RADIUS в сети для распределения нагрузки и обеспечений резервирования. Однако не все серверы RADIUS поддерживают совместно используемый кэш сеанса MAR. Только Версии ACS 5.4 и более поздний MAR поддержки. Перед этими версиями не возможно выполнить аутентификацию компьютера против одного сервера ACS и выполнить проверку подлинности пользователя против другого, поскольку они не соответствуют друг другу.

MAR и проводная беспроводная коммутация

Кэш MAR многих серверов RADIUS полагается на MAC-адрес. Это - просто таблица с MAC-адресом портативных ПК и меткой времени их последней успешной аутентификации компьютера. Таким образом, сервер может знать, был ли клиент машиной, аутентифицируемой в последнем X часов.

Однако, что происходит, если вы загружаете свой портативный ПК с проводным соединением (и поэтому делаете аутентификацию компьютера от вашего проводного MAC), и затем переключитесь к радио в течение дня? Сервер RADIUS не имеет никаких средств коррелировать ваш беспроводной MAC-адрес с вашим проводным MAC-адресом и знать, что вы были машиной, аутентифицируемой в прошлом X часов. Единственный путь состоит в том, чтобы выйти из системы и иметь поведение Microsoft Windows другая аутентификация компьютера через радио.

Решение

Среди многих других функций AnyConnect Cisco имеет преимущество предварительно сконфигурированных профилей, которые инициируют машину и проверку подлинности пользователя. Когда вы выходите из системы или перезагрузка, Однако с теми же ограничениями, как замечено с соискателем Microsoft Windows встречаются относительно аутентификации компьютера, только происходящей.

Кроме того, с Версиями AnyConnect 3.1 и позже, возможно выполнить EAP-FAST с объединением в цепочку EAP. Это - в основном одиночная аутентификация, куда вы передаете двух пар учетных данных, имени пользователя/пароля машины и имени пользователя / пароль, в то же время. ISE, тогда, более легко проверяет, что оба успешны. Без используемого кэша и никакая потребность получить предыдущий сеанс, это

представляет большую надежность.

Когда ПК загружается, AnyConnect передает аутентификацию компьютера только, потому что никакие сведения о пользователе не доступны. Однако на регистрационную информацию пользователя для входа, AnyConnect передает и машину и пользовательские учетные данные одновременно. Кроме того, если вы становитесь разъединенными или отключаете/повторно включаете кабель, и машина и учетные данные пользователя снова передаются на одиночной аутентификации EAP-FAST, которая отличается от более ранних версий AnyConnect без объединения в цепочку EAP.