Символический сервер RSA и использование протокола SDI для ASA и ACS

Содержание

Введение

Этот документ описывает процедуры устранения проблем для Менеджера Аутентификации RSA, который может быть интегрирован с устройством адаптивной защиты Cisco (ASA) и сервер Cisco Secure Access Control Server (ACS).

Менеджер Аутентификации RSA является решением, которое предоставляет Одноразовый пароль (OTP) для аутентификации. Тот пароль изменяется каждые 60 секунд и может использоваться только однажды. Это поддерживает оба маркера программного и аппаратного обеспечения.

Предварительные условия

Требования

Cisco рекомендует иметь базовые знания об этих темах:

- Конфигурация интерфейса командой строки Cisco ASA
- Конфигурация AcS Cisco

Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение Cisco ASA, Версия 8.4 и позже
- Cisco Secure ACS, Версия 5.3 и позже

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.

Теория

К серверу RSA можно обратиться с RADIUS или составляющим собственность протоколом RSA: SDI. И ASA и ACS могут использовать оба протокола (RADIUS, SDI) для доступа к RSA.

Помните, что RSA может быть интегрирован с защищенным мобильным клиентом Cisco AnyConnect Secure Mobility, когда используется программный маркер. Этот документ фокусируется исключительно на интеграции ACS и ASA. Для получения дополнительной информации о AnyConnect, обратитесь к Использованию раздела Аутентификации SDI Руководства администратора защищенного мобильного клиента Cisco AnyConnect Secure Mobility, Выпуска 3.1.

RSA через RADIUS

RADIUS имеет одно большое преимущество перед SDI. На RSA возможно назначить определенные профили (названный группами на ACS) пользователям. Тем профилям определили определенные атрибуты RADIUS. После успешной аутентификации RADIUS - Признает, что сообщение, возвращенное из RSA, содержит те атрибуты. На основе тех атрибутов ACS принимает дополнительные решения. Наиболее распространенный сценарий является решением использовать Сопоставление ACS Group для сопоставления определенных атрибутов RADIUS, отнесенных к профилю на RSA, определенной группе на ACS. С этой логикой возможно переместить целый процесс авторизации от RSA до ACS и все еще поддержать гранулированную логику, как на RSA.

RSA через SDI

SDI имеет два основных преимущества по RADIUS. Прежде всего, зашифрован целый сеанс. Вторыми являются содержательные возможности, которые предоставляет агент SDI:

это в состоянии определить, создан ли сбой, потому что аутентификация или авторизация отказала или потому что не был найден пользователь.

Эта информация используется ACS в действии для идентичности. Например, это могло продолжиться для "пользователя, не найденного", но отклонить для "подведенной аутентификации".

Существует еще одно различие между RADIUS и SDI. Когда Устройство Доступа к сети как ASA использует SDI, ACS выполняет только аутентификацию. Когда это использует RADIUS, ACS выполняет аутентификацию, авторизацию, считая (AAA). Однако это не большая разница. Возможно настроить SDI для аутентификации и RADIUS для того, чтобы составлять те же сеансы.

Протокол SDI

По умолчанию SDI использует Протокол UDP 5500. SDI использует ключ симметричного шифрования, подобный ключу RADIUS, для шифрования сеансов. Тот ключ сохранен в файле секретного узла и другой для каждого SDI - клиента. Тот файл развернут вручную или автоматически.

> **Примечание:** ACS/ASA не делает развертываний руководства по получению поддержки.

Для узла автоматического развертывания секретный файл загружен автоматически после первой успешной аутентификации. Секретный узел зашифрован с ключом, полученным из кода доступа пользователя и другой информации. Это создает некоторые возможные проблемы безопасности, таким образом, первая аутентификация должна быть выполнена локально, и использование зашифровало протокол (Secure Shell [SSH], не telnet), чтобы гарантировать, что атакующий не может перехватить и дешифровать тот файл.

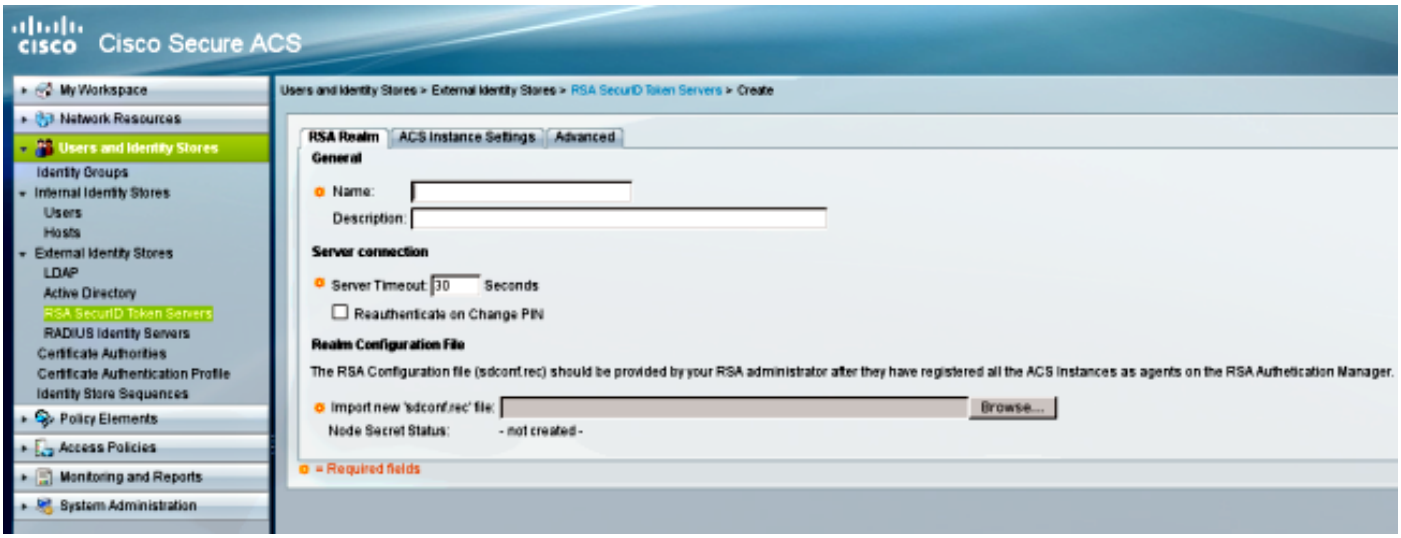
!--- конфигурацию

> **Примечания:**
>
> Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).
>
> Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**
>
> Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

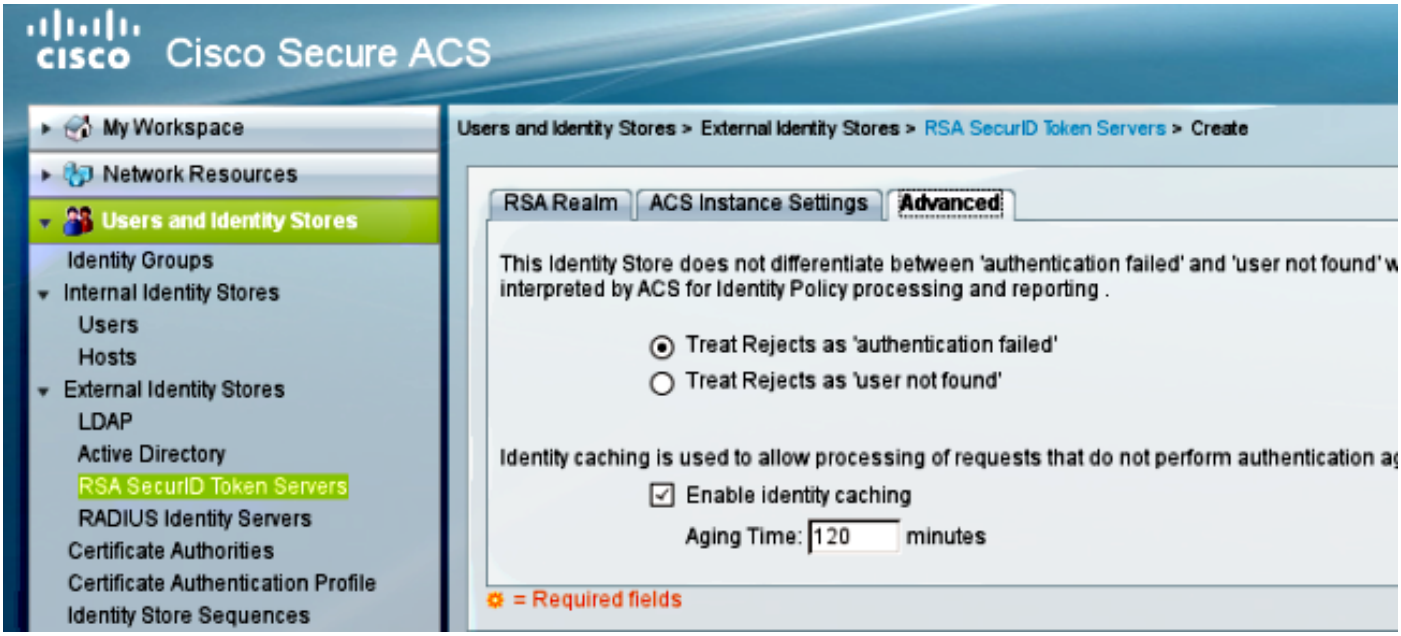
SDI на ACS

Это настроено в **Пользователях и Идентификационных Хранилищах> Внешнее хранилище идентификаторов> RSA Безопасный ID Символические серверы**.

RSA имеет множественные серверы реплик, такие как дополнительные серверы для ACS. Нет никакой потребности поместить все адреса там, просто **sdconf.rec** файл, предоставленный администратором RSA. Этот файл включает IP-адрес основного сервера RSA. После первого узла успешной аутентификации секретный файл загружен наряду с IP-адресами всех копий RSA.



Для дифференциации "пользователя, не найденного" от "ошибки проверки подлинности", выберите параметры настройки во **Вкладке Дополнительно**:



Также возможно изменить маршрутизацию по умолчанию (распределение нагрузки) механизмы между множественными серверами RSA (основной и копии). Измените его с **sdopts.rec** файлом, предоставленным администратором RSA. В ACS это загружено в **Пользователях и Идентификационных Хранилищах> Внешнее хранилище идентификаторов> RSA Безопасный ID Символические серверы> Параметры настройки Экземпляра ACS**.

Для кластерных развертываний должна быть реплицирована конфигурация. После первой успешной аутентификации каждый узел ACS использует свой собственный секретный узел,

загруженный от основного сервера RSA. Важно не забыть настраивать RSA для всех узлов ACS в кластере.

SDI на ASA

ASA не позволяет загрузку **sdconf.rec** файла. И, как ACS, это обеспечивает автоматическое развертывание только. ASA должен быть настроен вручную для обращения к основному серверу RSA. Пароль не необходим. После первого узла успешной аутентификации установлен секретный файл (.sdi файл на флэш-памяти), и защищены дальнейшие сеансы аутентификации. Также IP-адрес других серверов RSA загружен.

Например:

```
aaa-server SDI protocol sdi
aaa-server SDI (backbone) host 1.1.1.1
debug sdi 255
test aaa auth SDI host 1.1.1.1 user test pass 321321321
```

После успешной аутентификации, **СОИ протокола aaa-server показа** или **показывают**, что команда **<aaa-server-group> aaa-server** показывает все серверы RSA (если существуют несколько), в то время как **команда show run** показывает только основной IP - адрес:

```
bsns-asa5510-17# show aaa-server RSA
Server Group:   RSA
Server Protocol: sdi
Server Address: 10.0.0.101
Server port:    5500
Server status:  ACTIVE (admin initiated), Last transaction at
10:13:55 UTC Sat Jul 27 2013
Number of pending requests             0
Average round trip time                706ms
Number of authentication requests      4
Number of authorization requests       0
Number of accounting requests          0
Number of retransmissions              0
Number of accepts                      1
Number of rejects                      3
Number of challenges                   0
Number of malformed responses          0
Number of bad authenticators           0
Number of timeouts                     0
Number of unrecognized responses       0


SDI Server List:
       Active Address:         10.0.0.101
       Server Address:         10.0.0.101
       Server port:            5500
       Priority:               0
       Proximity:              2
       Status:                 OK
       Number of accepts                    0
       Number of rejects                    0
       Number of bad next token codes       0
       Number of bad new pins sent          0
       Number of retries                    0
       Number of timeouts                   0

       Active Address:         10.0.0.102
       Server Address:         10.0.0.102
```

```
Server port:            5500
Priority:               8
Proximity:              2
Status:                 OK
Number of accepts                       1
Number of rejects                       0
Number of bad next token codes          0
Number of bad new pins sent             0
Number of retries                       0
Number of timeouts                      0
```

Устранение неполадок

Этот раздел обеспечивает информацию, которую вы можете использовать для того, чтобы устранить неисправность в вашей конфигурации.

Никакая настройка агента на RSA

Во многих случаях после того, как вы устанавливаете новый ASA или изменяете IP-адрес ASA, легко забыть вносить те же изменения на RSA. IP-адрес Агента на RSA должен быть обновлен для всех клиентов, которые обращаются к RSA. Затем тайна нового узла генерируется. То же применяется к ACS, особенно к вторичным узлам, потому что у них есть другие IP-адреса, и RSA должен доверять им.

Поврежденный секретный узел

Иногда секретный файл узла на ASA или RSA становится поврежденным. Затем лучше удалять настройку агента на RSA и добавлять его снова. Также необходимо сделать, тот же процесс на ASA/ACS - удаляет и добавляет конфигурацию снова. Кроме того, удалите .sdi файл на флэш-памяти, так, чтобы на следующей аутентификации, был установлен новый .sdi файл. Автоматические развертывания секретного узла должны произойти, как только это завершено.

Узел в приостановленном режиме

Иногда один из узлов находится в приостановленном режиме, который не вызван никаким ответом от того сервера:

```
asa# show aaa-server RSA
<.....output ommited"
SDI Server List:
Active Address: 10.0.0.101
Server Address: 10.0.0.101
Server port: 5500
Priority: 0
Proximity: 2
  Status:                  SUSPENDED
```

В приостановленном режиме ASA не пытается передать любые пакеты к тому узлу; это должно иметь статус **OK** для этого. Сервер с ошибкой помещен в активный режим снова после таймера простоя. Для получения дополнительной информации обратитесь к разделу командного режима оживления в Справочнике по командам Серии Cisco ASA, 9.1

руководствах.

В таких сценариях, лучше удалять и добавлять конфигурацию AAA-server для той группы для инициирования того сервера в активный режим снова.

Блокированная учетная запись

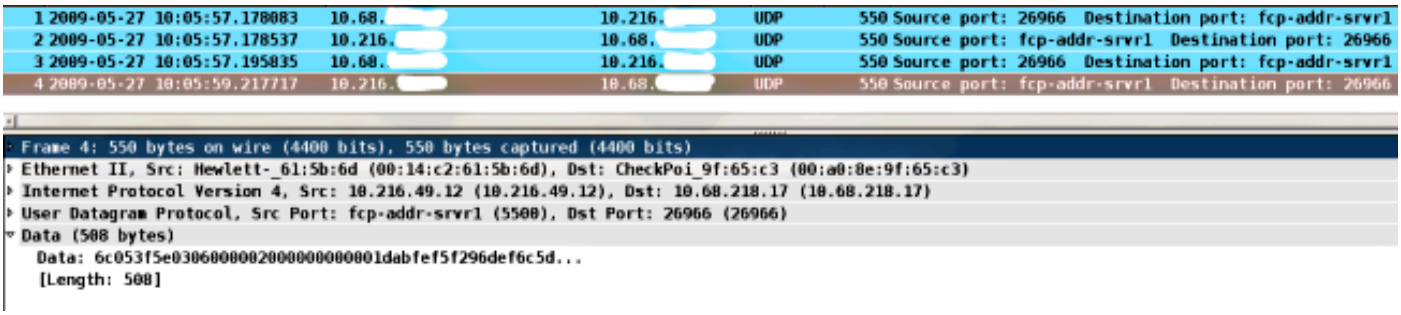
После множественных повторных попыток RSA мог бы блокировать с учетной записи. Это легко проверено на RSA с отчётами. На ASA/ACS, сообщает, только показывают "ошибку проверки подлинности".

Проблемы Maximum Transition Unit (MTU) и фрагментация

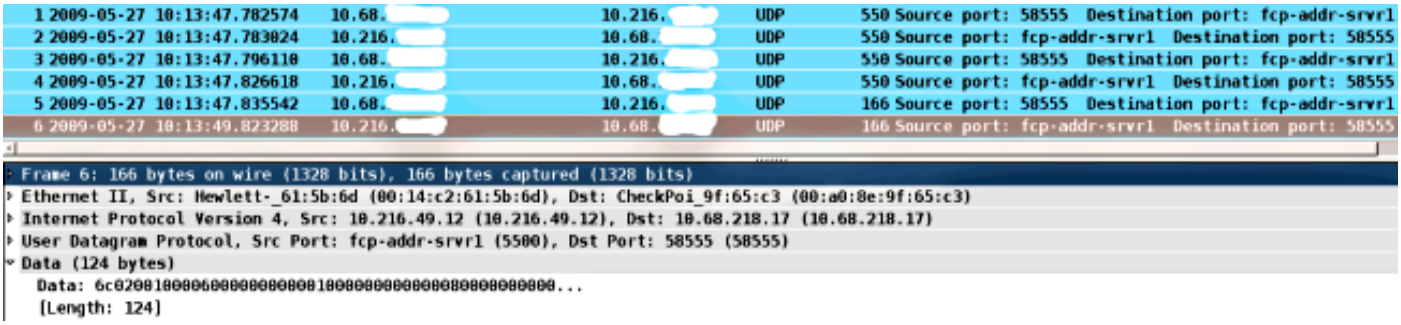
SDI использует UDP в качестве транспорта, не обнаружения пути MTU. Также трафику UDP не установили бит "Не фрагментировать" (DF) по умолчанию. Иногда для больших пакетов, могли бы быть проблемы фрагментации. Легко осуществить сниффинг трафика на RSA (и устройство и Виртуальная машина [VM], используют Windows и используют Wireshark). Завершите тот же процесс на ASA/ACS и выдержите сравнение. Кроме того, тестовый RADIUS или WebAuthentication на RSA для сравнения его с SDI (для сужения проблемы).

Пакеты и отладки для ACS

Поскольку информационное наполнение SDI зашифровано, единственный способ устранить неполадки перехватов состоит в том, чтобы сравнить размер ответа. Если это меньше, чем 200 байтов, могла бы быть проблема. Типичный обмен SDI включает четыре пакета, каждый из которых составляет 550 байтов, но это могло бы измениться с версией сервера RSA:



В случае проблем это обычно - больше чем четыре пакета обмененные и меньшие размеры:



Кроме того, журналы ACS довольно ясны. Вот типичный SDI, входит в систему ACS:

```
EventHandler,11/03/2013,13:47:58:416,DEBUG,3050957712,Stack: 0xa3de560
Calling backRSAIDStore: Method MethodCaller<RSAIDStore, RSAAgentEvent> in
thread:3050957712,EventStack.cpp:242

AuthenSessionState,11/03/2013,13:47:58:416,DEBUG,3050957712,cntx=0000146144,
sesn=acs-01/150591921/1587,user=mickey.mouse,[RSACheckPasscodeState
::onEnterState],RSACheckPasscodeState.cpp:23

EventHandler,11/03/2013,13:47:58:416,DEBUG,3002137488,Stack: 0xa3de560
Calling RSAAgent:Method MethodCaller<RSAAgent, RSAAgentEvent> in thread:
3002137488,EventStack.cpp:204

RSAAgent,11/03/2013,13:47:58:416,DEBUG,3002137488,cntx=0000146144,sesn=
acs-01/150591921/1587,user=mickey.mouse,[RSAAgent::handleCheckPasscode],
RSAAgent.cpp:319

RSASessionHandler,11/03/2013,13:47:58:416,DEBUG,3002137488,[RSASessionHandler::
checkPasscode] call AceCheck,RSASessionHandler.cpp:251

EventHandler,11/03/2013,13:48:00:417,DEBUG,2965347216,Stack: 0xc14bba0
Create newstack, EventStack.cpp:27

EventHandler,11/03/2013,13:48:00:417,DEBUG,3002137488,Stack: 0xc14bba0 Calling
RSAAgent: Method MethodCaller<RSAAgent, RSAServerResponseEvent> in
thread:3002137488,EventStack.cpp:204

RSAAgent,11/03/2013,13:48:00:417,DEBUG,3002137488,cntx=0000146144,sesn=acs-01
/150591921/1587,user=mickey.mouse,[RSAAgent::handleResponse] operation completed
with ACM_OKstatus,RSAAgent.cpp:237

EventHandler,11/03/2013,13:48:00:417,DEBUG,3002137488,Stack: 0xc14bba0
EventStack.cpp:37

EventHandler,11/03/2013,13:48:00:417,DEBUG,3049905040,Stack: 0xa3de560 Calling
back RSAIDStore: Method MethodCaller<RSAIDStore, RSAAgentEvent> in thread:
3049905040,EventStack.cpp:242

AuthenSessionState,11/03/2013,13:48:00:417,DEBUG,3049905040,cntx=0000146144,sesn=
acs-01/150591921/1587,user=mickey.mouse,[RSACheckPasscodeState::onRSAAgentResponse]
Checkpasscode succeeded, Authentication passed,RSACheckPasscodeState.cpp:55
```

Дополнительные сведения

- Менеджер аутентификации RSA ресурсы
- Поддержка RSA/СЕРВЕРА SDI раздел Руководство по настройке Cisco ASA 5500 с помощью CLI, 8.4 и 8.6
- Сервер RSA SecurID раздел Руководство пользователя для системы управления доступом Cisco Secure Access Control System 5.4
- Cisco Systems – техническая поддержка и документация