Содержание

Введение

Эта статья объясняет подробные данные относительно реализаций EAP-FAST на Менеджере доступа к сети (NAM) AnyConnect Cisco и платформе Identity Services Engine (ISE). Это далее объясняет, как определенные функции сотрудничают, и предоставляет типичные варианты использования и примеры.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о платформе EAP и методах EAP-FAST
- Базовые знания о платформе Identity Services Engine (ISE)
- Базовые знания о NAM AnyConnect и Редакторе Профиля
- Базовые знания о конфигурации Cisco Catalyst для сервисов 802.1x

Используемые компоненты

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

- Windows 7 с защищенным мобильным клиентом Cisco AnyConnect Secure Mobility, выпуском 3.1 и 4.0
- Cisco Catalyst 3750X переключается с программным обеспечением 15.2.1 и позже
- Cisco ISE, выпуск 1.4

Теория

Фазы

EAP-FAST является гибким методом EAP, который позволяет обоюдную проверку подлинности соискателя и сервера. Это подобно PEAP EAP, но, как правило, не требует использования клиента или даже серверных сертификатов. Одно преимущество EAP-FAST является способностью объединить несколько серверов проверки подлинности в цепочку (использующий множественные внутренние методы) и связать его криптографически вместе (Объединение в цепочку EAP). Внедрения Cisco используют это для проверок подлинности пользователя и аутентификаций компьютера.

EAP-FAST использует учетные данные для защищенного доступа (PAC) для быстрого установления туннеля TLS (резюме сеанса), или авторизовать пользователя/машину (пропустите внутренний метод проверки подлинности).

Существует 3 фазы для EAP-FAST:

- фаза 0 (инициализация PAC)
- фаза 1 (установка туннеля TLS)
- фаза 2 (Аутентификация)

EAP-FAST поддерживает PAC меньше и основанный на PAC диалог. Основанный на PAC состоит из инициализации PAC и основанной на PAC аутентификации. Инициализация PAC может основываться на анонимном или аутентифицируемом сеансе TLS.

PAC

PAC является Учетными данными Защищенного доступа, генерируемыми сервером и предоставленными клиенту. Это состоит из:

- Ключ PAC (случайное секретное значение, используемое для получения ведущего устройства TLS и ключей сеанса)
- Непрозрачный PAC (ключ PAC + идентичность пользователя - все зашифрованные главным ключом сервера EAP-FAST)
- Информация PAC (идентичность сервера, таймеры TTL)

Сервер, выполняя PAC зашифрует ключ PAC и идентичность с помощью главного ключа сервера EAP-FAST (который является непрозрачным PAC), и передает целый PAC клиенту. Это не поддерживает/хранит никакую другую информацию (кроме главного ключа, который является тем же для всех PAC).

Как только непрозрачный PAC получен, он дешифрован с помощью главного ключа сервера EAP-FAST и проверен. Ключ PAC используется для получения ведущего устройства TLS и ключей сеанса для сокращенного туннеля TLS.

Когда предыдущий главный ключ истекает, генерируются новые главные ключи сервера EAP-FAST. В некоторых случаях главный ключ может быть отозван.

Существует несколько типов того, что PAC был используемым в настоящее время:

- Туннельный PAC: используемый для установки туннеля TLS (без потребности клиента или серверного сертификата). Передаваемый в Сообщении приветствия клиента TLS
- PAC машины: используемый для установки туннеля TLS и непосредственной авторизации машины. Передаваемый в Сообщении приветствия клиента TLS
- PAC Авторизации пользователя: используемый для непосредственной проверки подлинности пользователя (пропускают внутренний метод), если позволено сервером. Передаваемый в туннеле TLS с помощью TLV.
- PAC Авторизации машины: используемый для непосредственной аутентификации компьютера (пропускают внутренний метод), если позволено сервером. Передаваемый в туннеле TLS с помощью TLV.
- PAC Trustsec: используемый для авторизации при выполнении связанный со средой или обновление политики.

Все те PAC обычно отправляются автоматически в фазе 0. Часть PAC (Туннель, Машина, Trustsec) может быть также отправлена вручную.

Когда генерируются PAC

- Туннельный PAC: настроенный после успешной аутентификации (внутренний метод) , если не используемый ранее.
- PAC авторизации: настроенный после успешной аутентификации (внутренний метод) , если не используемый ранее.
- PAC машины: настроенный после успешной аутентификации компьютера (внутренний метод), если не используемый ранее и когда не используется PAC Авторизации. Когда Туннельный PAC истечет, это будет proviosioned; однако, не, когда истекает PAC Авторизации. Когда Объединение в цепочку EAP будет включено или отключено, это будет настроено.

Примечание:

Каждая инициализация PAC требует успешной аутентификации кроме следующего варианта использования: авторизованный пользователь просит PAC Машины для машины, которая не имеет AD учетной записи.

Следующая таблица суммирует инициализацию и упреждающую функциональность обновления:

Тип PAC	Туннель v1/v1a/CTS	Машина	Authorization
Предоставьте PAC на запросе на инициализации	да	только на аутентифицируемой инициализации	только на аутентифицируемой инициализации и ес
Предоставьте PAC на запросе на аутентификации	да	да	Туннельный PAC запрашивают также только если это не использовалось на э аутентификации
Упреждающее обновление	да	нет	нет
При переключении на PAC, настраивающий после подведенной основанной на PAC аутентификации (например, когда PAC истекается),	отклонение и Дон? t предоставляют новый	отклонение и Дон? t предоставляют новый	отклонение и Дон? t предоставляют новы
ACS поддержки 4.x PAC	для Туннельного PAC v1/v1a	да	нет

ACS главного ключа сервера EAP-FAST 4.x по сравнению с ACS 5x и ISE

Существует небольшое различие в обработке Главного ключа при сравнении ACS 4.x и ISE

Функция	ACS 4.1.2	ACS 5.x / ISE
Главный ключ	Главный ключ имеет TTL, может быть активным, исключен или с истекшим сроком	Главный ключ автоматически генерируется от прототипа в каждом настроенном периоде времени. Определенный Главный ключ всегда доступен и затем никогда не истечен
Обновление PAC	Обновление PAC передается сервером, когда PAC истекается, пока не истекается Главный ключ, используемый для шифрования PAC	Обновление PAC передается сервером после первой успешной аутентификации, которая выполнена в определенном настраиваемом периоде времени перед моментом истечения PAC.

Другими словами, ISE будет поддерживать все old master ключи и генерировать новый по

умолчанию один раз в неделю. Поскольку Главный ключ не может истечь, только TTL PAC будет проверен.

Период генерации Главного ключа ISE настроен от *администрирования-> Параметры настройки-> Протокол-> EAP-FAST-> Параметры настройки EAP-FAST.*

Резюме сеанса

Это - важный компонент, обеспечивая Туннельное использование PAC. Это обеспечивает туннельный пересмотр TLS без использования сертификатов.

Существует два типа резюме сеанса для EAP-FAST: Состояние сервера базировалось и не сохраняющий состояние (основанный PAC).

Состояние сервера

Стандартный TLS базировался, метод основывается на TLS SessionID, кэшируемом на сервере. Клиент, передающий Сообщение приветствия клиента TLS, подключает SessionID для возобновления сеанса. Сеанс только используется для инициализации PAC при использовании анонимного туннеля TLS:

Source	Destination	Protocol	Length	Info	User-Name
10.62.148.109	10.48.17.14	RADIUS	378	Access-Request(1) (id=9, l=	anonymous
10.48.17.14	10.62.148.109	RADIUS	86	Access-Reject(3) (id=9, l=4	
10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=30, l	anonymous
10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=30	
10.62.148.109	10.48.17.14	RADIUS	510	Access-Request(1) (id=31, l	anonymous

```
  Length: 138
  Type: Flexible Authentication via Secure Tunneling EAP (EAP-FAST) (43)
▷ EAP-TLS Flags: 0x01
▽ Secure Sockets Layer
  ▽ TLSv1 Record Layer: Handshake Protocol: Client Hello
      Content Type: Handshake (22)
      Version: TLS 1.0 (0x0301)
      Length: 127
    ▽ Handshake Protocol: Client Hello
        Handshake Type: Client Hello (1)
        Length: 123
        Version: TLS 1.0 (0x0301)
      ▷ Random
        Session ID Length: 32
        Session ID: 9a344ae351082ec6dbafb8509cf99b4fa664574b6272f876...
        Cipher Suites Length: 52
      ▷ Cipher Suites (26 suites)
        Compression Methods Length: 1
      ▷ Compression Methods (1 method)
```

Не сохраняющий состояние (основанный PAC)

PAC Авторизации пользователя/Машины используется для хранения предыдущих состояний проверки подлинности и авторизация для узла.

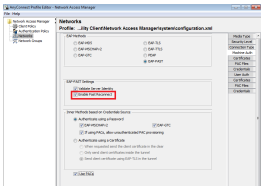
Резюме клиентской стороны основывается на RFC 4507. Сервер не должен кэшировать данные; вместо этого клиент подключает PAC в Сообщении приветствия клиента TLS расширение SessionTicket. В свою очередь PAC проверен сервером. Пример на основе Туннельного PAC поставил к серверу:

	Source	Destination	Protocol	Length	Info	User-Name
23	10.62.148.109	10.48.17.14	RADIUS	301	Access-Request(1) (id=91, l=259)	anonymous
24	10.48.17.14	10.62.148.109	RADIUS	193	Access-Challenge(11) (id=91, l=151)	
25	10.62.148.109	10.48.17.14	RADIUS	666	Access-Request(1) (id=92, l=624)	anonymous
26	10.48.17.14	10.62.148.109	RADIUS	311	Access-Challenge(11) (id=92, l=269)	
27	10.62.148.109	10.48.17.14	RADIUS	437	Access-Request(1) (id=93, l=395)	anonymous
28	10.48.17.14	10.62.148.109	RADIUS	226	Access-Challenge(11) (id=93, l=184)	
29	10.62.148.109	10.48.17.14	RADIUS	468	Access-Request(1) (id=94, l=426)	anonymous
30	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=94, l=216)	
31	10.62.148.109	10.48.17.14	RADIUS	516	Access-Request(1) (id=95, l=474)	anonymous
32	10.48.17.14	10.62.148.109	RADIUS	258	Access-Challenge(11) (id=95, l=216)	
33	10.62.148.109	10.48.17.14	RADIUS	452	Access-Request(1) (id=96, l=410)	anonymous

```
▽ TLSv1 Record Layer: Handshake Protocol: Client Hello
    Content Type: Handshake (22)
    Version: TLS 1.0 (0x0301)
    Length: 281
  ▽ Handshake Protocol: Client Hello
      Handshake Type: Client Hello (1)
      Length: 277
      Version: TLS 1.0 (0x0301)
    ▷ Random
      Session ID Length: 0
      Cipher Suites Length: 52
    ▷ Cipher Suites (26 suites)
      Compression Methods Length: 1
    ▷ Compression Methods (1 method)
      Extensions Length: 184
    ▽ Extension: SessionTicket TLS
        Type: SessionTicket TLS (0x0023)
        Length: 180
        Data (180 bytes)
▷ AVP: l=18  t=Message-Authenticator(80): 0cb2477c076ea96d3ba150245e6291e8
```

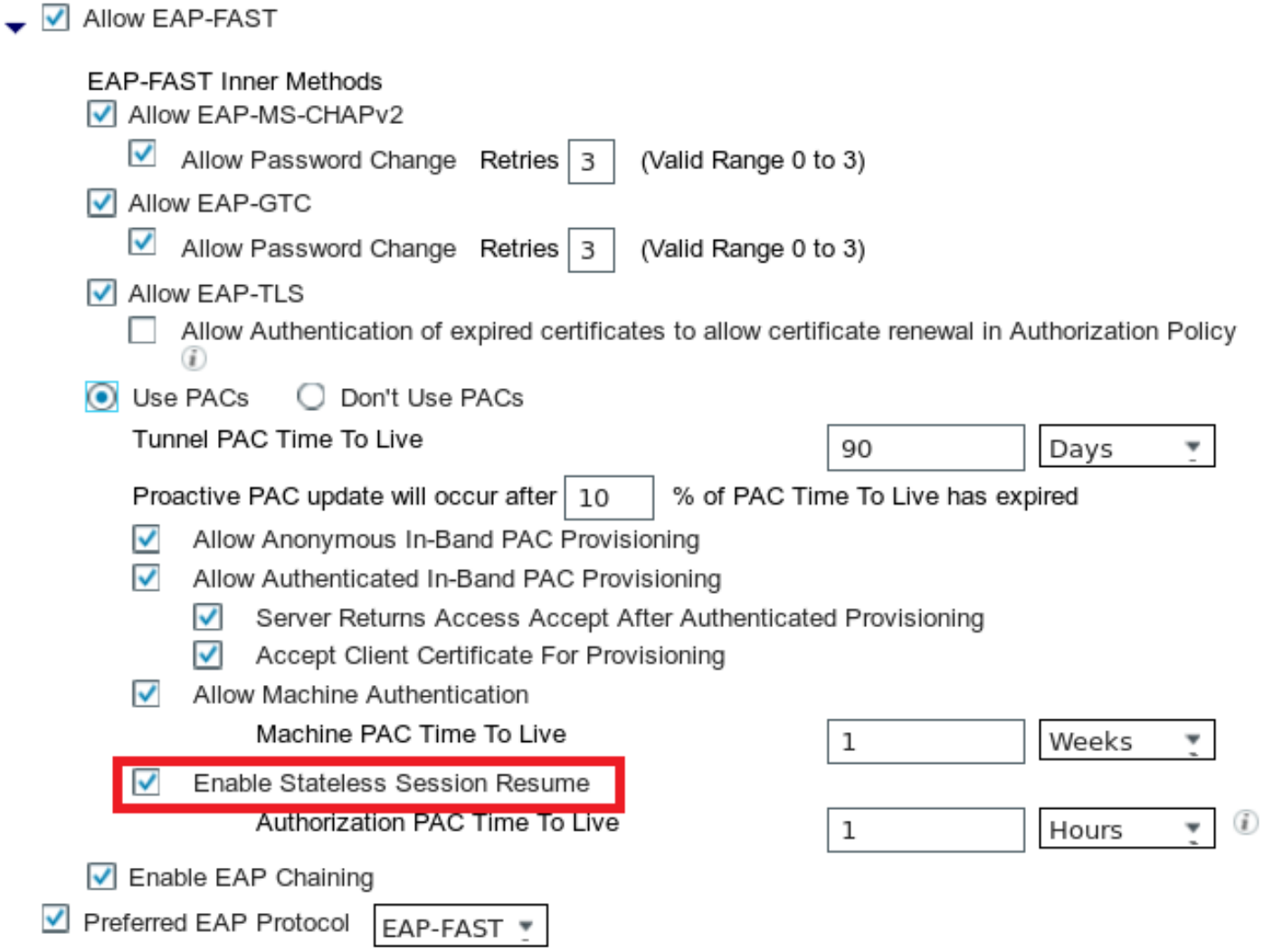
Реализация NAM AnyConnect

Это включено на клиентской стороне (NAM AnyConnect) через Быстрый Повторно соединяются - но это используется для управления только использованием PAC авторизации.



С отключенной установкой NAM будет все еще использовать туннельный PAC для построения туннеля TLS (никакие необходимые сертификаты). Однако это не будет использовать PAC авторизации для выполнения непосредственного пользователя и авторизации машины. В результате фаза 2 с внутренним методом будет всегда требоваться.

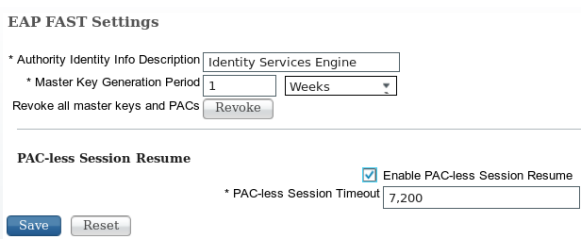
ISE имеет опцию для включения Резюме Сеанса Не сохраняющего состояние. И как на NAM это только для PAC Авторизации. Туннельное использование PAC управляется с опциями "Use PACs".



Если опция будет включена, NAM попытается использовать PAC. Если "не Используют PAC", настроен в ISE, и ISE получает Туннельный PAC в расширении TLS, об ошибке слежения сообщат, и Сбой EAP возвращен:

вставьте здесь

В ISE также необходимо включить резюме сеанса на основе TLS SessionID (от Глобальных параметров настройки EAP-FAST). Это отключено по умолчанию:



Следует иметь в виду, что может использоваться только один тип резюме сеанса. SessionID базировался, используется только для развертываний PAC меньше, основанный RFC 4507 используется только для развертываний PAC.

Инициализация PAC (фаза 0)

PAC могут быть автоматически настроены в phase0. Фаза 0 состоит из:

- Установка туннеля TLS
- Аутентификация (внутренний метод)

PAC отправлены после успешной аутентификации в туннеле TLS через TLV PAC (и Подтверждение TLV PAC)

Анонимный туннель TLS

Для развертываний без инфраструктуры PKI возможно использовать анонимный туннель TLS. Анонимный туннель TLS будет создан с помощью набора шифров Диффи-Хеллмана - без потребности сервера или сертификата клиента. Этот подход является склонным для man в Средних атаках (олицетворение).

Для использования этой опции NAM требует следующей настроенной опции:

"Если PAC использования позволяют не прошедший поверку подлинности PAC настраивать" (который целесообразен только для основанного на пароле внутреннего метода, потому что без инфраструктуры PKI не возможно использовать основанный на сертификате внутренний метод).

Кроме того, ISE будет нужно следующее, настроенное в соответствии с Опознавательными Разрешенными протоколами:

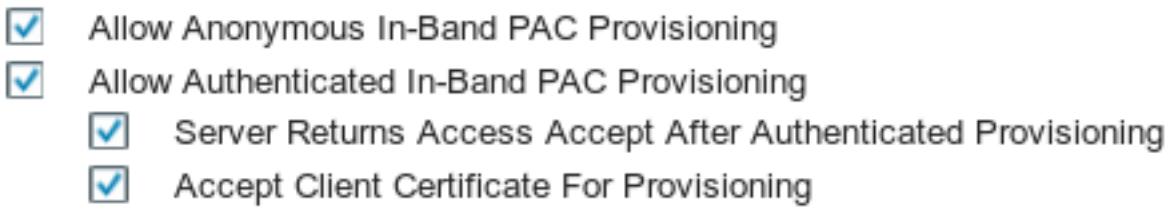
"Позвольте анонимную внутриполосную инициализацию PAC"

Анонимная внутриполосная инициализация PAC используется в развертываниях TrustSec NDAC (сеанс EAP-FAST, о котором выполняют согласование между сетевыми устройствами).

Аутентифицируемый туннель TLS

Это - самая безопасная и рекомендуемая опция. Туннель TLS создан на основе серверного сертификата, который проверен соискателем. Это требует инфраструктуры PKI на стороне сервера только, которая требуется для ISE (на NAM, возможно отключить опцию "Validate Server Identity".

Для ISE существует два дополнительных параметра:



Обычно, после инициализации PAC, Access-Reject должен быть передан, вынудив соискателя повторно аутентифицировать PAC использования. Но так как PAC были отправлены в туннеле TLS с аутентификацией, возможно сократить весь процесс и возвратить Access-Accept сразу после инициализации PAC.

Вторая опция создает туннель TLS на основе сертификата клиента (это требует развертываний PKI на оконечных точках). Это позволяет туннелю TLS быть созданным с обоюдной проверкой подлинности, которая пропускает внутренний метод и идет непосредственно в фазу инициализации PAC. Важно быть осторожным здесь - иногда , соискатель представит сертификат, которому не доверяет ISE (предназначенный для других целей), и сеанс откажет.

Объединение в цепочку EAP

Позволяет проверку подлинности пользователя и аутентификацию компьютера в одном сеансе Радиуса/EAP. Множественные методы EAP могут быть объединены в цепочку вместе. После того, как первая аутентификация (как правило, машина) закончилась успешно, сервер передаст TLV Промежуточного Результата (в туннеле TLS) указание на успех. Тот TLV должен сопровождаться Крипто-Обязательным Запросом TLV. Cryptobinding используется, чтобы доказать, что оба сервер и узел участвовали в определенной последовательности аутентификаций. Процесс Cryptobinding использует материал для кодирования от фазы 1 и фазы 2. Кроме того, еще один TLV подключен: Информационное наполнение EAP - это инициирует новый сеанс (как правило, для пользователя). Как только сервер RADIUS (ISE) получает Крипто-Обязательный Ответ TLV и проверяет его, придерживающееся покажут в журнале, и следующий метод EAP попробуют (как правило, за проверку подлинности пользователя):

Если cryptobinding проверка отказывает, целые сбои сеанса EAP. : если одна из аутентификаций в отказавшем тогда администратору настраивать множественные результаты объединения в цепочку на основе Условия Авторизации NetworkAccess:EapChainingResult, это прекрасно все еще - в результате ISE позволяет

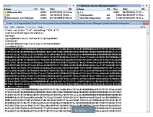
- No chaining
- User and machine both succeeded
- User failed and machine succeeded
- User succeeded and machine failed

Когда проверка подлинности пользователя EAP-FAST и аутентификация компьютера включены, объединение в цепочку EAP включено на NAM автоматически.

Объединение в цепочку EAP должно быть настроено в ISE.

Где хранятся файлы PAC

По умолчанию Туннель и PAC Машины сохранены в C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\internalConfiguration.xml в разделах <учетные данные>. Те сохранены в зашифрованной форме.

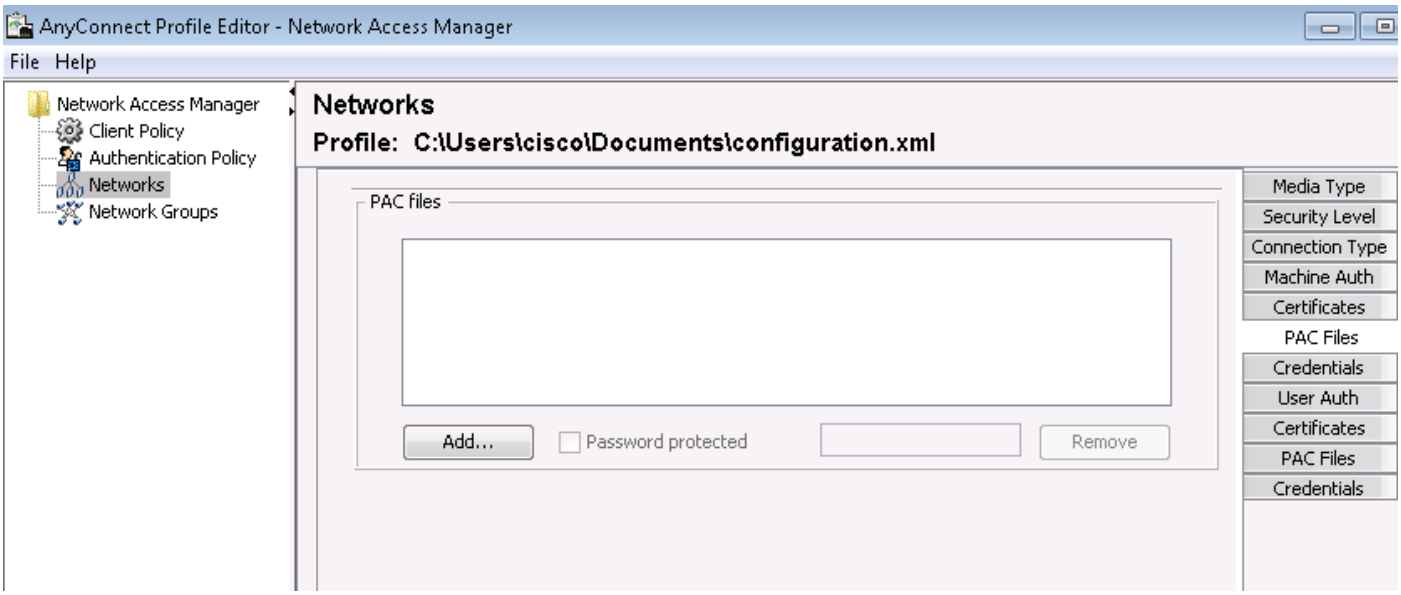


PAC авторизации сохранены только в памяти и удалены после перезагрузки или перезапуска сервиса NAM.

Сервисный перезапуск требуется, чтобы удалять PAC Туннельного или Машины.

AnyConnect NAM 3.1 по сравнению с 4.0

AnyConnect 3.x редактор профиля NAM позволил администратору настраивать PAC вручную. Эта функция была удалена из AnyConnect 4.x редактор профиля NAM.

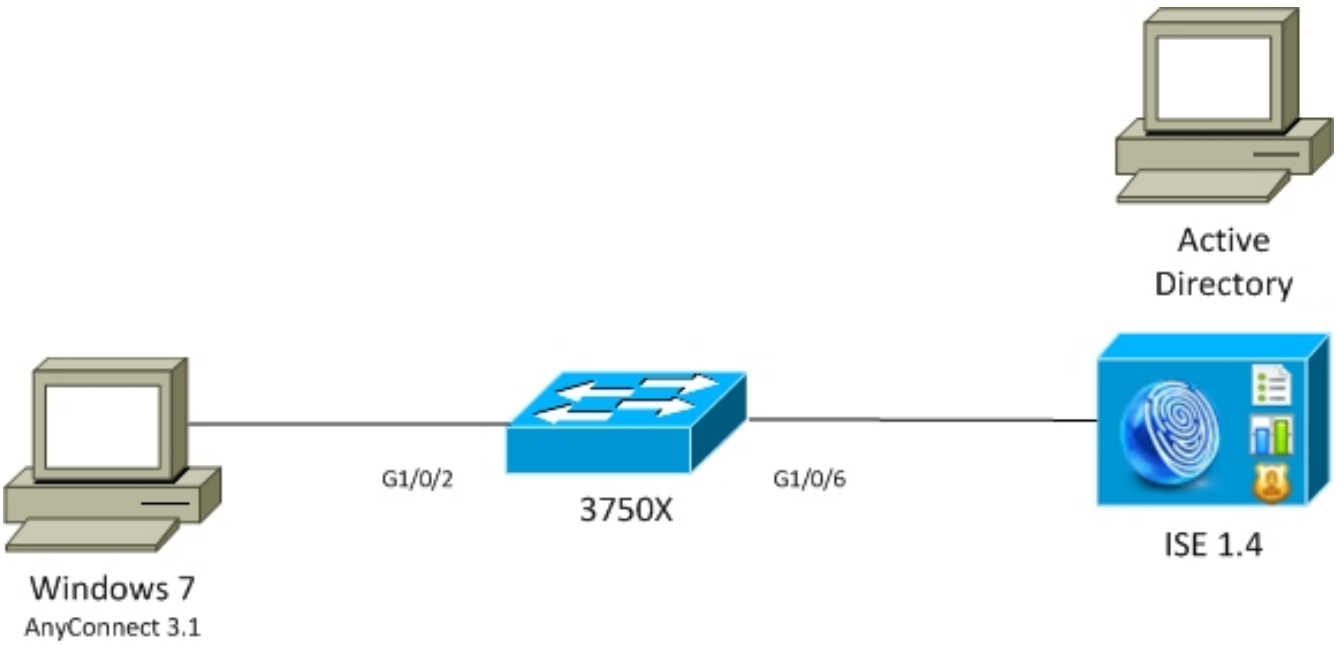


Решение удалить ту функциональность основывается на CSCuf31422 и CSCua13140.

Примеры

Схема сети

Все примеры были протестированы с помощью следующей топологии сети. То же применяется также при использовании радио.



Быстрый EAP без объединения в цепочку EAP с пользователем и PAC машины

По умолчанию EAP_chaining отключен на ISE. Однако все другие опции включены включая PAC Машины и Авторизации. У соискателя уже есть допустимый Машина и Туннельный PAC. В этом потоке будет две отдельных аутентификации - один для машины и один для пользователя - с отдельным входом в систему ISE. Основные шаги, как зарегистрировано ISE. Первая аутентификация (машина):

- Соискатель передает Сообщение приветствия клиента TLS с PAC Машины.
- Сервер проверяет PAC Машины и создает туннель TLS (никакие используемые сертификаты).
- Сервер проверяет PAC Машины и выполняет поиск учетной записи в Active Directory и пропускает внутренний метод.

```
12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800 Extracted first TLS record; TLS handshake started
12174 Received Machine PAC
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded
12132 EAP-FAST built PAC-based tunnel for purpose of authentication

24351 Account validation succeeded
24420 User's Attributes retrieval from Active Directory succeeded - example.com
22037 Authentication Passed
12124 EAP-FAST inner method skipped

11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept
```

Вторая аутентификация (пользователь):

- Соискатель передает Сообщение приветствия клиента TLS с Туннельным PAC.
- Сервер проверяет PAC и создает туннель TLS (никакие используемые сертификаты).
- Поскольку у соискателя нет PAC Авторизации, внутренний метод (MSCHAP EAP) используется для аутентификации.

```
12102 Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800 Extracted first TLS record; TLS handshake started
12175 Received Tunnel PAC
12805 Extracted TLS ClientHello message
12806 Prepared TLS ServerHello message
12801 Prepared TLS ChangeCipherSpec message

12816 TLS handshake succeeded
12132 EAP-FAST built PAC-based tunnel for purpose of authentication
12125 EAP-FAST inner method started
11806 Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402 User authentication against Active Directory succeeded - example.com
22037 Authentication Passed

11503 Prepared EAP-Success
11002 Returned RADIUS Access-Accept
```

В "Других Атрибутах" раздел подробного отчета в ISE, ниже приводится известный и проверками подлинности пользователя и аутентификациями компьютера:

Быстрый EAP с объединением в цепочку EAP с PAC Быстро Повторно

соединяются

В этом потоке у соискателя уже есть допустимый Туннельный PAC наряду с PAC Авторизации Пользовательского и Машины:

- Соискатель передает Сообщение приветствия клиента TLS с Туннельным PAC.
- Сервер проверяет PAC и создает туннель TLS (никакие используемые сертификаты).
- ISE запускает Объединение в цепочку EAP, соискатель подключает PAC Авторизации для пользователя и Машины с помощью TLV в туннеле TLS.
- ISE проверяет PAC Авторизации (никакой внутренний необходимый метод), проверяет, что учетные записи существуют в Active Directory (никакая дополнительная аутентификация), возвращает успех.

```
12102   Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800   Extracted first TLS record; TLS handshake started
12175   Received Tunnel PAC
12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12801   Prepared TLS ChangeCipherSpec message

12816   TLS handshake succeeded
12132   EAP-FAST built PAC-based tunnel for purpose of authentication
12209   Starting EAP chaining
12210   Received User Authorization PAC
12211   Received Machine Authorization PAC

24420   User's Attributes retrieval from Active Directory succeeded - example.com
22037   Authentication Passed

24439   Machine Attributes retrieval from Active Directory succeeded - example.com
22037   Authentication Passed

11503   Prepared EAP-Success
11002   Returned RADIUS Access-Accept
```

В "Других Атрибутах" раздел подробного отчета в ISE, ниже приводится обращенный внимание:

Кроме того, и пользователь и учетные данные машины включены в тот же журнал, как замечено ниже:

Быстрый EAP с объединением в цепочку EAP без PAC

В этом потоке NAM настроен для не использования PAC, ISE также настроен для не использования PAC (но с Объединением в цепочку EAP)

- Соискатель передает Сообщение приветствия клиента TLS без Туннельного PAC.
- Сервер отвечает информационными наполнениями Сертификата и Запроса сертификата TLS.
- Соискатель должен доверять серверному сертификату, не передаст сертификата клиента (информационное наполнение сертификата является нулем), туннель TLS создан.
- ISE отправляет запрос TLV для сертификата клиента в туннеле TLS, но соискатель не делает (не необходимо иметь его для продолжения).
- Запускает Объединение в цепочку EAP для пользователя, с помощью внутреннего метода с аутентификацией MSCHAPv2.
- Продолжает аутентификацию компьютера, с помощью внутреннего метода с

аутентификацией MSCHAPv2.
- Никакие PAC не настраиваются.

Быстрый EAP с EAP, объединяющим истечение PAC авторизации в цепочку

В этом потоке Соискатель имеет допустимый Туннельный PAC, но истек PAC Авторизации:

- Соискатель передает Сообщение приветствия клиента TLS с Туннельным PAC.
- Сервер проверяет PAC и создает туннель TLS (никакие используемые сертификаты).
- ISE запускает Объединение в цепочку EAP, соискатель подключает PAC Авторизации для Пользователя и Машины с помощью TLV в туннеле TLS.
- Поскольку PAC истекаются, внутренний метод и для пользователя и для машины запущен (MSCHAP EAP).
- Как только обе аутентификации успешны, и пользователь и PAC Авторизации машины настроены.

```
12102   Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800   Extracted first TLS record; TLS handshake started
12175   Received Tunnel PAC
12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12801   Prepared TLS ChangeCipherSpec message

12816   TLS handshake succeeded
12132   EAP-FAST built PAC-based tunnel for purpose of authentication
12209   Starting EAP chaining
12227   User Authorization PAC has expired - will run inner method
12228   Machine Authorization PAC has expired - will run inner method
12218   Selected identity type 'User'

11806   Prepared EAP-Request for inner method proposing EAP-MSCHAP with challenge

24402   User authentication against Active Directory succeeded - example.com
22037   Authentication Passed

12219   Selected identity type 'Machine'

24470   Machine authentication against Active Directory is successful - example.com
22037   Authentication Passed

12171   Successfully finished EAP-FAST user authorization PAC provisioning/update
12179   Successfully finished EAP-FAST machine authorization PAC provisioning/update

11503   Prepared EAP-Success
11002   Returned RADIUS Access-Accept
```

Быстрый EAP с EAP, объединяющим туннельный PAC в цепочку, истек

В этом потоке, когда никакой допустимый туннельный PAC не существует, происходит полное согласование TLS с внутренней фазой.

- Соискатель передает Сообщение приветствия клиента TLS без Туннельного PAC.
- Сервер отвечает информационными наполнениями Сертификата и Запроса сертификата TLS.
- Соискатель должен доверять серверному сертификату, не передаст сертификат клиента (информационное наполнение сертификата является нулем), созданный туннель TLS.
- ISE отправляет запрос TLV для сертификата клиента в туннеле TLS, но соискатель не делает (не необходимо иметь его для продолжения).

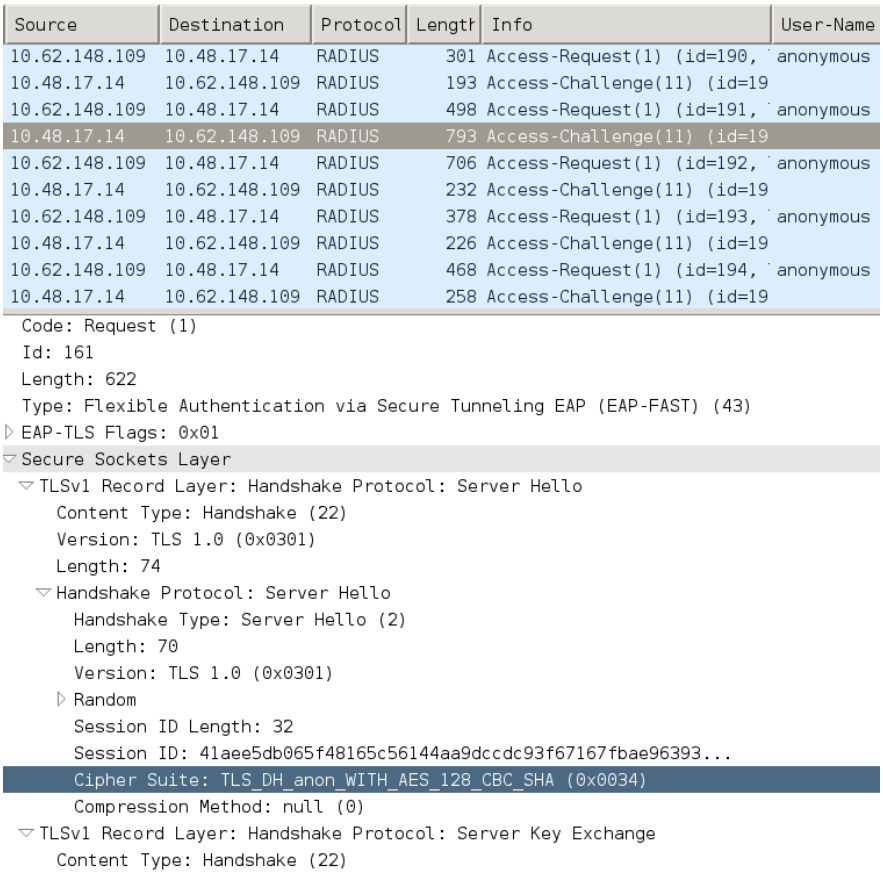
- Запускает Объединение в цепочку EAP для пользователя, с помощью внутреннего метода с аутентификацией MSCHAPv2.
- Продолжает аутентификацию компьютера, с помощью внутреннего метода с аутентификацией MSCHAPv2.
- Успешно настроенный все PAC (включил в config ISE).

Быстрый EAP с объединением в цепочку EAP и анонимной туннельной инициализацией PAC TLS

В этом потоке ISE и NAM анонимный туннель TLS настроен для инициализации PAC (ISE аутентифицировался, туннель TLS для инициализации PAC отключен), запрос инициализации PAC похож:

- Соискатель передает Сообщение приветствия клиента TLS без множественного ciphersuites.
- Сервер отвечает TLS Приветствие сервера и TLS анонимные шифры Диффи-Хеллмана (например, TLS_DH_anon_WITH_AES_128_CBC_SHA).
- Соискатель принимает его, и анонимный туннель TLS создан (никакие сертификаты, которыми обмениваются).
- Запускает Объединение в цепочку EAP для пользователя, с помощью внутреннего метода с аутентификацией MSCHAPv2.
- Продолжает аутентификацию компьютера, с помощью внутреннего метода с аутентификацией MSCHAPv2.
- Так как анонимный туннель TLS является созданными PAC Авторизации, не позволены.
- Отклонение радиуса возвращено, чтобы вынудить соискателя повторно аутентифицироваться (использование обеспеченного PAC).

Захваты пакета Wireshark для анонимного согласования туннеля TLS:



Быстрый EAP с проверкой подлинности пользователя объединения в цепочку EAP только

В этом потоке настроен NAM AnyConnect с EAP-FAST и Пользователем (EAP-TLS) и Аутентификация компьютера (EAP-TLS). Компьютер с операционной системой Windows загружен, но не предоставлены учетные данные пользователя. Коммутатор инициирует сеанс 802.1x, NAM должен ответить, однако, учетные данные пользователя еще не предоставлены, (никакой доступ к пользовательскому хранилищу и сертификату) поэтому. проверка подлинности пользователя откажет, в то время как машина будет успешна - ISE authz условие "

- Соискатель передает Сообщение приветствия клиента TLS с PAC Машины.
- Сервер отвечает Спецификацией Шифра Изменения TLS - туннель TLS сразу является сборкой на основе того PAC.
- ISE инициирует Объединение в цепочку EAP и выяснение идентичности пользователя.
- Соискатель предоставляет идентичность машины вместо этого (пользователь, еще не готовый), EAP-TLS концов внутренний метод.
- ISE просит идентичность пользователя снова, соискатель не может предоставить его.
- ISE передает TLV с промежуточным результатом = сбой (для проверки подлинности пользователя).
- ISE возвращает заключительное сообщение об успешном завершении EAP, подведенный пользователь Access:EapChainingResult EQUALS Сети условия ISE и машина, за которой следуют

```
12102   Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800   Extracted first TLS record; TLS handshake started
12174   Received Machine PAC

12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12801   Prepared TLS ChangeCipherSpec message
12802   Prepared TLS Finished message

12816   TLS handshake succeeded
12132   EAP-FAST built PAC-based tunnel for purpose of authentication

12209   Starting EAP chaining
12218   Selected identity type 'User'

12213   Identity type provided by client is not equal to requested type
12215   Client suggested 'Machine' identity type instead

12104   Extracted EAP-Response containing EAP-FAST challenge-response
12523   Extracted EAP-Response/NAK for inner method requesting to use EAP-TLS instead

12805   Extracted TLS ClientHello message
12806   Prepared TLS ServerHello message
12807   Prepared TLS Certificate message
12809   Prepared TLS CertificateRequest message

12816   TLS handshake succeeded
12509   EAP-TLS full handshake finished successfully

22070   Identity name is taken from certificate attribute
15013   Selected Identity Source - Test-AD
24323   Identity resolution detected single matching account
22037   Authentication Passed

12202   Approved EAP-FAST client Authorization PAC request
12218   Selected identity type 'User'
12213   Identity type provided by client is not equal to requested type
12216   Identity type provided by client was already used for authentication
12967   Sent EAP Intermediate Result TLV indicating failure

12179   Successfully finished EAP-FAST machine authorization PAC provisioning/update
12106   EAP-FAST authentication phase finished successfully
11503   Prepared EAP-Success
11002   Returned RADIUS Access-Accept
```

Быстрый EAP с объединением в цепочку EAP и противоречивыми анонимными параметрами туннеля TLS

В этом потоке ISE настроен для PAC, настраивающего только через анонимный туннель TLS, но NAM использует аутентифицируемый туннель TLS, придерживающееся будет зарегистрировано ISE:

```
12102   Extracted EAP-Response containing EAP-FAST challenge-response and accepting EAP-FAST as negotiated
12800   Extracted first TLS record; TLS handshake started
12805   Extracted TLS ClientHello message
12814   Prepared TLS Alert message
12817   TLS handshake failed
12121   Client didn't provide suitable ciphers for anonymous PAC-provisioning

11504   Prepared EAP-Failure
11003   Returned RADIUS Access-Reject
```

Это происходит , когда NAM пытается создать аутентифицируемый туннель TLS с, он - speciphic шифры TLS - и те не приняты ISE, который настроен для анонимного туннеля TLS (принимающий только шифры DH)

Устранение неполадок

ISE

Для подробных журналов отладки Aaa во время выполнения должны быть включены на соответствующем узле PSN. Ниже несколько журналов в качестве примера от prrt-server.log:

Генерация PAC машины:

Утверждение запроса PAC:

Проверка PAC:

Пример успешной сводки для генерации PAC:

Пример успешной сводки для проверки PAC:

NAM AnyConnect

Журналы DART от NAM предоставляют следующие детали:

Пример для сеанса Объединения в цепочку EAP non, Аутентификация компьютера без быстрого повторно соединяется:

Пример поиска PAC Авторизации (аутентификация компьютера для сеанса Объединения в цепочку EAP non):

Все состояния внутреннего метода (для MSCHAP) могут быть проверены от журналов ниже:

NAM позволяет конфигурацию расширенной характеристики входа в систему, которая перехватит все пакеты EAP и сохранит их в pcap файле. Это особенно полезно для Запуска Перед функциональностью Входа в систему (Пакеты EAP перехвачены даже для

аутентификаций, которые происходят перед пользовательским входом в систему). Для функции активация спрашивают вашего инженера TAC.

Ссылки

- Руководство администратора Защищенного мобильного клиента Cisco AnyConnect Secure Mobility, конфигурация EAP-FAST Выпуска 4.0
- Руководство администратора Платформы Cisco Identity Services Engine, рекомендации EAP-FAST Выпуска 1.4
- Руководства по дизайну платформы Cisco Identity Services Engine
- Развертывание объединения в цепочку EAP с NAM AnyConnect и Cisco ISE
- Cisco Systems – техническая поддержка и документация