

Настройте ISE 2.2 IPSEC для обеспечения NAD (ASA) связь

Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Общие сведения](#)

[Архитектура IPsec ISE](#)

[Настройка](#)

[Схема сети](#)

[Конфигурация ASA](#)

[Настройте интерфейсы ASA](#)

[Настройте политику IKEv1 и включите IKEv1 на внешнем интерфейсе](#)

[Настройте туннельную группу \(профиль прямого соединения локальных сетей\)](#)

[Настройте ACL для трафика VPN интереса](#)

[Настройте набор преобразований IKEv1](#)

[Настройте Криптокарту и Примените ее к Интерфейсу](#)

[Окончательная конфигурация ASA](#)

[Конфигурация ISE](#)

[Настройте IP-адрес на ISE](#)

[Добавьте NAD к группе IPsec на ISE](#)

[Включите IPSEC на ISE](#)

[Проверка](#)

[ASA](#)

[ESR](#)

[ISE](#)

[Устранение неполадок](#)

[Настройте от узла к узлу FlexVPN \(DVTI к криптокарте\) между NAD и ISE 2.2](#)

[Конфигурация ASA](#)

[Конфигурация ESR на ISE](#)

[Вопросы проектирования FlexVPN](#)

Введение

Этот документ описывает, как настроить и устранить неполадки IPSEC RADIUS для обеспечения Идентификационного механизма сервиса (ISE) Cisco 2.2 - связь Устройства доступа к сети (NAD). Трафик сервера RADIUS должен быть зашифрован в от узла к узлу (LAN-LAN) Версия 1 и 2 Обмена ключами между сетями IPsec (IKEv1 и IKEv2) туннель между Устройством адаптивной защиты (ASA) и ISE. Этот документ не покрывает часть конфигурации VPN SSL AnyConnect.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- ISE
- Cisco ASA
- Общие понятия IPSec
- Общие понятия RADIUS

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- 5515-X ASA Серии Cisco , который работает под управлением ПО версии 9.4 (2) 11
- Идентификационная версия 2.2 Механизма Сервиса Cisco
- Windows 7 Service Pack 1

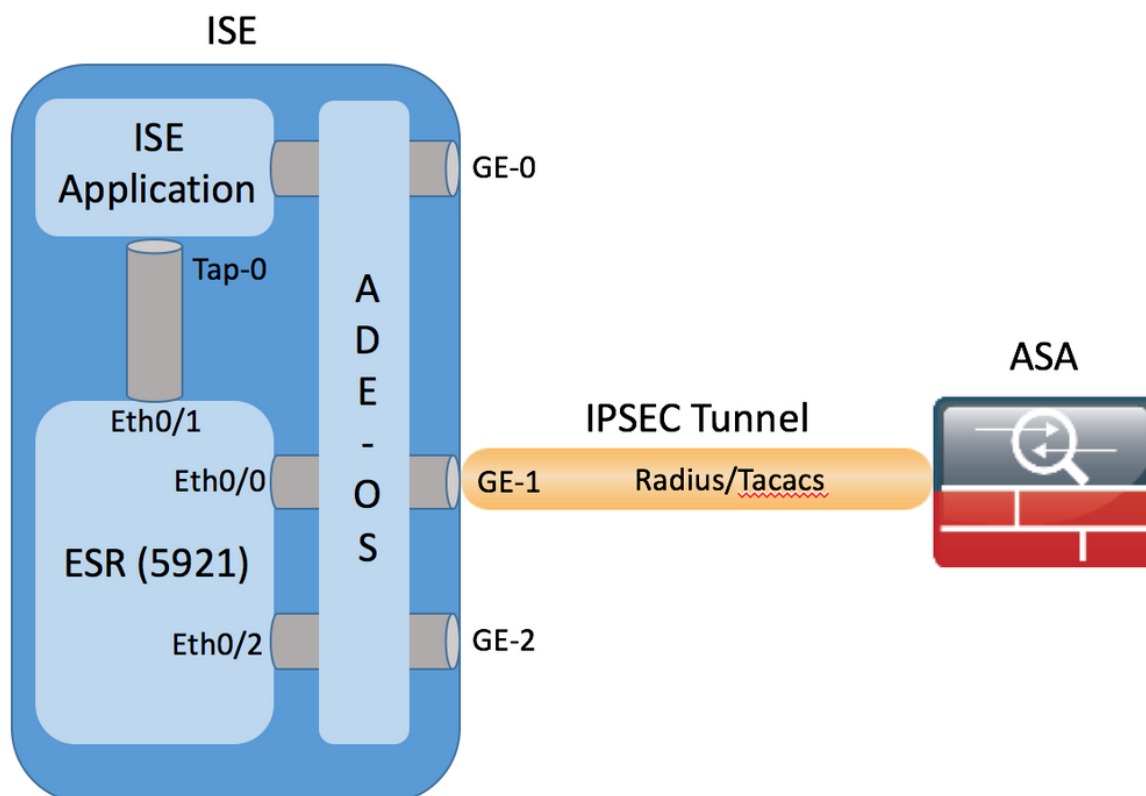
Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Цель к защищенным протоколам, которые используют опасный хэш MD5, Радисус и TACACS с IPSec. Примите это во внимание:

- Cisco ISE поддерживает IPSec в Туннеле и Транспортных режимах.
- При включении IPSec на интерфейсе Cisco ISE Туннель IPSec создан между Cisco ISE и NAD для обеспечения связи.
- Можно определить предварительный общий ключ или использовать сертификаты X.509 для Аутентификации IPSec.
- IPSec может быть включен на Eth1 через интерфейсы Eth5. Можно настроить IPSec только на одном интерфейсе Cisco ISE на PSN.

Архитектура IPSec ISE



Как только зашифрованные пакеты получены ESR интерфейса GE 1 ISE, перехватывает их на интерфейсе Eth0/0.

```
interface Ethernet0/0
description e0/0->connection to external NAD
ip address 10.48.26.170 255.255.255.0
ip nat outside
ip virtual-reassembly in
no ip route-cache
crypto map radius
```

ESR дешифрует их, и согласно предварительно сконфигурированному NAT правила выполняют переадресацию. При выходе (к NAD) пакеты RADIUS/TACACS преобразованы в адрес интерфейса Ethernet0/0 и зашифрованы впоследствии.

```
ip nat inside source list 1 interface Ethernet0/0 overload
ip nat inside source static udp 10.1.1.2 1645 interface Ethernet0/0 1645
ip nat inside source static udp 10.1.1.2 1646 interface Ethernet0/0 1646
ip nat inside source static udp 10.1.1.2 1812 interface Ethernet0/0 1812
ip nat inside source static udp 10.1.1.2 1813 interface Ethernet0/0 1813
ip nat inside source static tcp 10.1.1.2 49 interface Ethernet0/0 49
access-list 1 permit 10.1.1.0 0.0.0.3
```

Пакеты, которые предназначены к интерфейсу Eth0/0 на портах RADIUS/TACACS, должны быть forwarded через интерфейс Eth0/1 к 10.1.1.2 IP-адресам, которые являются внутренним адресом ISE. Конфигурация ESR Eth0/1

```
interface Ethernet0/1
description e0/1->tap0 internal connection to ISE
ip address 10.1.1.1 255.255.255.252
ip nat inside
ip virtual-reassembly in
no ip route-cache
```

Конфигурация ISE внутреннего Ответителя 0 интерфейсов:

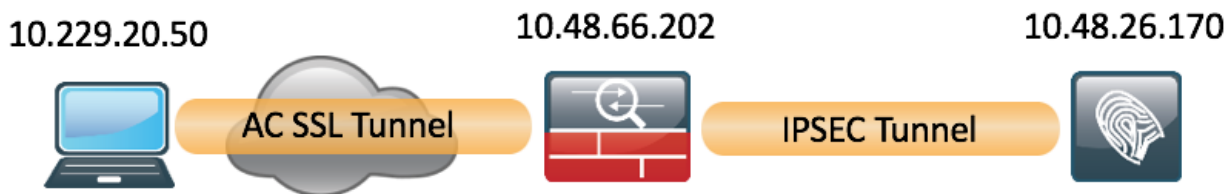
```
ISE22-1ek/admin# show interface | b tap0
tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.1.1.2 netmask 255.255.255.252 broadcast 10.1.1.3
    inet6 fe80::6c2e:37ff:fe5f:b609 prefixlen 64 scopeid 0x20<link>
    ether 6e:2e:37:5f:b6:09 txqueuelen 500 (Ethernet)
    RX packets 81462 bytes 8927953 (8.5 MiB)
    RX errors 0 dropped 68798 overruns 0 frame 0
    TX packets 105 bytes 8405 (8.2 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

Настройка

В этом разделе описывается завершить CLI ASA и конфигурации ISE.

Схема сети

Сведения в этом документе используют эту сетевую установку:



Конфигурация ASA

Настройте интерфейсы ASA

Если интерфейс/интерфейсы ASA не настроен, гарантирует настройку, по крайней мере, IP-адреса, имени интерфейса и уровня безопасности:

```
interface GigabitEthernet0/0
  nameif outside
  security-level 100
  ip address 10.48.66.202 255.255.254.0
```

Настройте политику IKEv1 и включите IKEv1 на внешнем интерфейсе

Для настройки политики Протокола ISAKMP для соединений IKEv1 введите крипто-ikev1 команду <priority> политики:

```
crypto ikev1 policy 20
  authentication pre-share
  encryption aes
  hash sha
  group 5
  lifetime 86400
```

Примечание: Когда обе из политики от двух узлов содержит ту же аутентификацию,

шифрование, хэш и значения параметра Диффи-Хеллмана, соответствие политики IKEv1 существует. Для IKEv1 политика удаленного узла должна также задать срок действия, меньше чем или равный сроку действия в политике, которую передает инициатор. Если сроки службы не идентичны, то ASA использует более короткий срок действия.

Необходимо включить IKEv1 на интерфейсе, который завершает VPN-туннель. Как правило, это - внешняя сторона (или *общественность*) интерфейс. Для включения IKEv1 войдите, **крипто-ikev1** выполняют команду `<interface-name>` в режиме глобальной конфигурации:

```
crypto ikev1 enable outside
```

Настройте туннельную группу (профиль прямого соединения локальных сетей)

Для туннеля между локальными сетями (LAN-to-LAN) тип профиля подключения является **ipsec-l2l**. Для настройки общего ключа IKEv1 введите режим конфигурации *атрибутов IPsec туннельной группы*:

```
crypto ikev1 enable outside
```

Настройте ACL для трафика VPN интереса

ASA использует Списки контроля доступа (ACL) для дифференциации трафика, который должен быть защищен с IP - безопасным шифрованием от трафика, который не требует защиты. Это защищает исходящие пакеты, которые совпадают с Системой управления заявки о разрешении на природопользование (ACE), и гарантирует, что входящие пакеты, которые совпадают с ACE разрешения, имеют защиту.

```
access-list 101 extended permit ip host 10.48.66.202 host 10.48.26.170
```

Примечание: ACL для трафика VPN использует источник и IP - адреса назначения после Технологии NAT. Единственный трафик, зашифрованный в этом случае, является трафиком между ASA и ISE.

Настройте набор преобразований IKEv1

Набор преобразований IKEv1 является комбинацией протоколов безопасности и алгоритмов, которые определяют способ, которым ASA защищает данные. Во время согласований IPsec Security Association (SA) узлы должны определить набор преобразований или предложение, которое является тем же для обоих из узлов. ASA тогда применяет набор преобразований, с которым совпадают, или предложение для создания SA, который защищает потоки данных в списке доступа для той криптокарты.

Для настройки набора преобразований IKEv1 введите **крипто-команду ipsec ikev1 transform-set**:

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

Настройте Криптокарту и Примените ее к Интерфейсу

Криптокарта определяет Политику IPsec, которая будет договорной в КОНТЕКСТЕ БЕЗОПАСНОСТИ IPSEC, и включает:

- Список доступа для определения пакетов, которые IP - безопасное соединение разрешает и защищает
- Одноранговая идентификация
- Локальный адрес для Трафика IPSec
- Наборы преобразований IKEv1

Например:

```
crypto ipsec ikev1 transform-set SET2 esp-aes esp-sha-hmac
```

Можно тогда применить криптокарту к интерфейсу:

```
crypto map MAP interface outside
```

Окончательная конфигурация ASA

Вот окончательная конфигурация на ASA:

```
crypto map MAP interface outside
```

Конфигурация ISE

Настройте IP-адрес на ISE

Адрес должен быть настроен на интерфейсом GE1-GE5 от CLI, GE0 не поддерживается.

```
crypto map MAP interface outside
```

Примечание: Перезапуска приложения после IP-адреса настроены на интерфейсе:
% Изменение IP-адреса могло бы заставить сервисы ISE перезапускать
Продолжить изменение IP-адреса? Y/N [N]: Y

Добавьте NAD к группе IPSec на ISE

Перейдите к **администрированию**> **Сетевые ресурсы**> **Сетевые устройства**. Щелкните по **Add**. Гарантируйте настройку Названия, IP-адреса, Общего секретного ключа. Для завершения Туннеля IPSec от NAD выбирают **YES against IPSEC Network Device Group**.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network devices

Default Device

Device Security Settings

Network Devices List > EK_ASA

Network Devices

Name

Description

* IP Address: /

* Device Profile

Model Name

Software Version

* Network Device Group

Device Type

IPSEC

Location

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol

* Shared Secret

CoA Port

Как только NAD добавлен, дополнительный маршрут должен быть создан на ISE, чтобы гарантировать, что Трафик сервера RADIUS проходит ESR и зашифрован:

```
crypto map MAP interface outside
```

Включите IPSEC на ISE

Перейдите к **администрированию**> Система> Параметры настройки. Щелкните по **Radius** и далее на **IPSEC**. Выберите PSN (Single/Multiple/All), Выбирают опцию Enable, выбирают Интерфейс и Выбирают Authentication Method. **Нажмите Save**. Сервисы перезапускают на выбранном узле на этом этапе.

Обратите внимание, что после того, как конфигурация интерфейса командой строки ISE перезапуска сервисов показывает настраиваемый интерфейс без IP-адреса и в состоянии завершения работы, это ожидается, поскольку ESR (маршрутизатор Embedded Services) берет под свой контроль интерфейс ISE.

```
crypto map MAP interface outside
```

Как только сервисы перезапущены, функциональность ESR добавлена. Для входа в систему к ESR вводят esg в командной строке:

```
crypto map MAP interface outside
```

ESR, придумывает следующее крипто - настройку:

```
crypto map MAP interface outside
```

Из-за ASA не поддерживает sha256, хеширующий algorithm, дополнительная настройка требуется на ESR совпасть с политикой IKEv1 для 1-й и 2-й фазы IPSEC. Настройте политику ISAKMP и набор преобразований, для соответствия с настроенными на ASA:

```
crypto map MAP interface outside
```

Удостоверьтесь, что ESR имеет маршрут для отсылки зашифрованных пакетов:

```
crypto map MAP interface outside
```

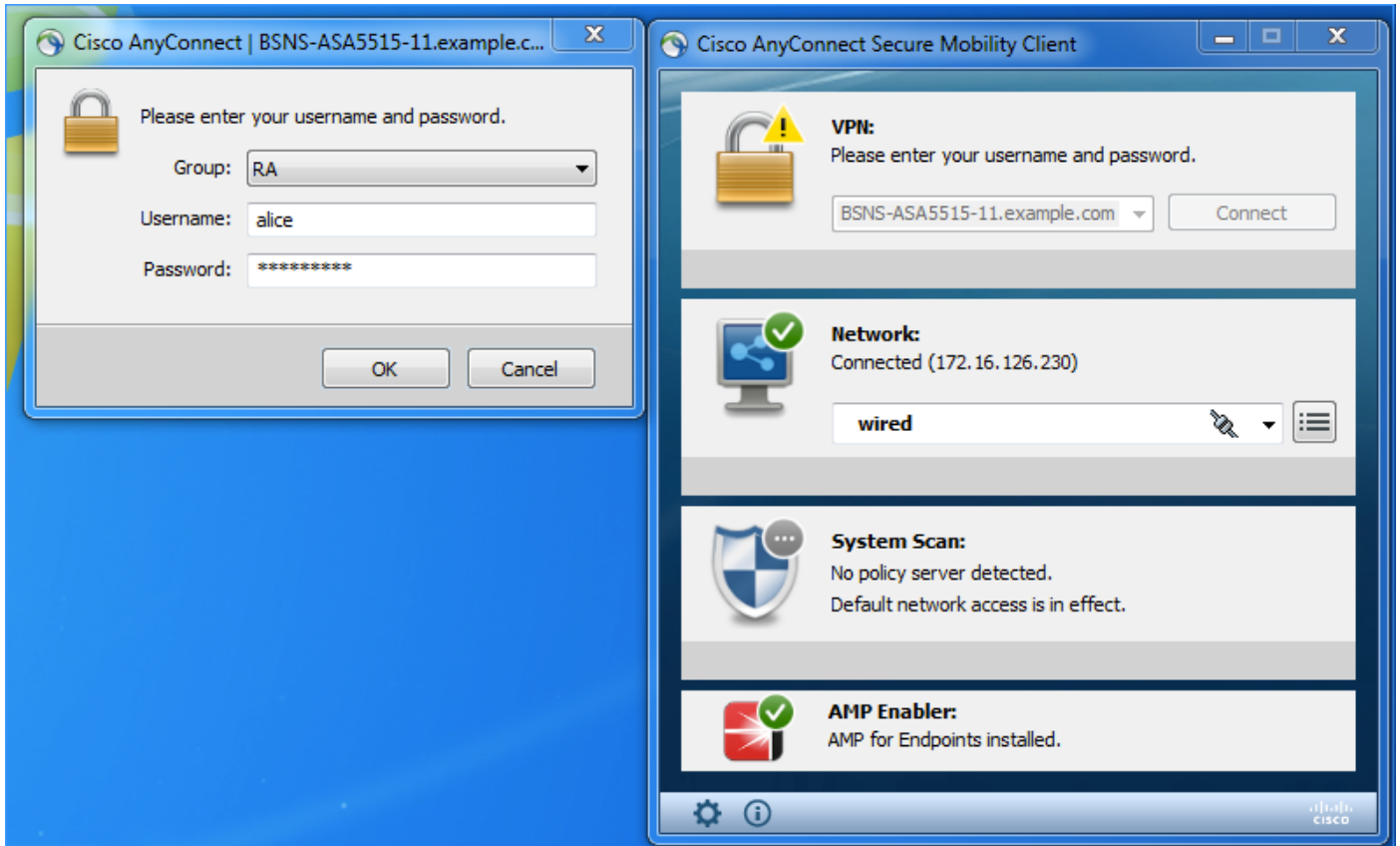
Проверка

ASA

Прежде чем клиенты Anyconnect соединятся, ASA не имеет никакого сеанса шифрования:

```
crypto map MAP interface outside
```

Клиентские подключения через Клиента AnyConnect VPN Client, поскольку источник аутентификационной информации ISE 2.2 используется.



ASA передает Пакет RADIUS, который инициирует установление сеанса VPN, когда-то туннель является следующим результатом, замечен на ASA, и это подтверждает, что фаза 1 туннеля подключена:

```
crypto map MAP interface outside
```

Фаза 2 подключена, и пакеты зашифрованы и дешифрованы:

```
crypto map MAP interface outside
```

ESR

Те же выходные данные могут быть проверены на ESR, фаза 1 подключена:

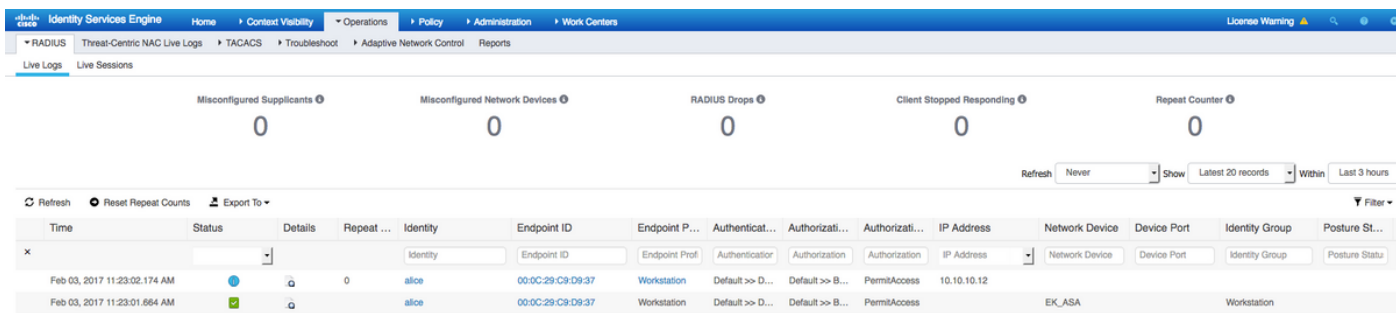
```
crypto map MAP interface outside
```

Фаза 2 подключена, пакеты зашифрованы и дешифрованы успешно:

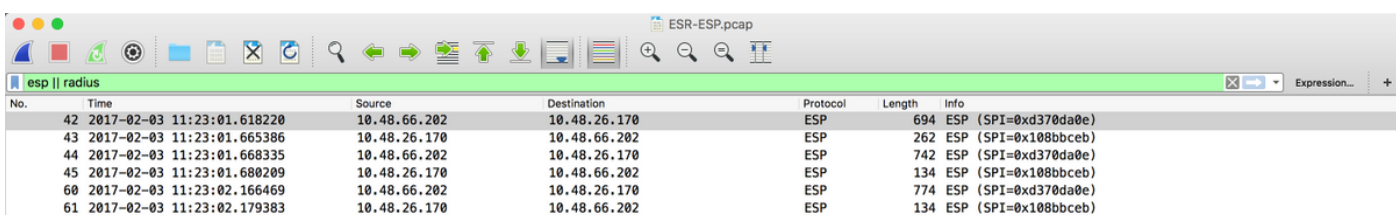
```
crypto map MAP interface outside
```

ISE

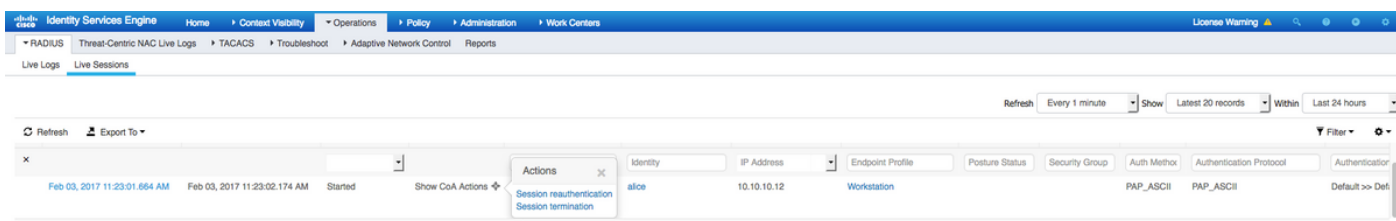
Оперативная Аутентификация указывает на обычную аутентификацию PAP_ASCII:



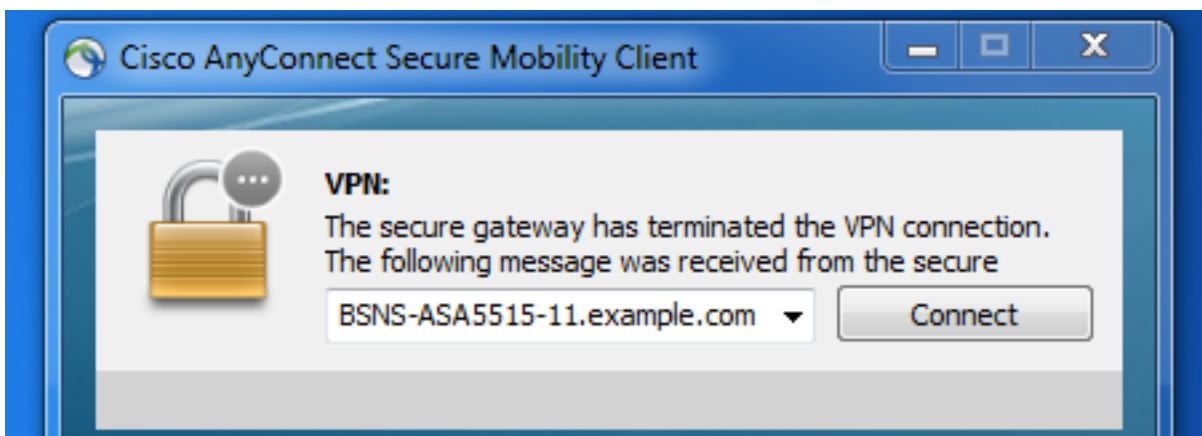
Перехватывает взятый, интерфейс GE1 ISE и фильтруемый с ESP или Радиусом, подтверждает, что нет никакого Радиуса в открытом тексте, и весь трафик зашифрован:



Также возможно передать зашифрованные пакеты от ISE - изменения авторизации (CoA) - как только туннель в порядке:



В данном примере было выполнено Завершение сеанса, и клиент VPN был разъединен в результате:



Устранение неполадок

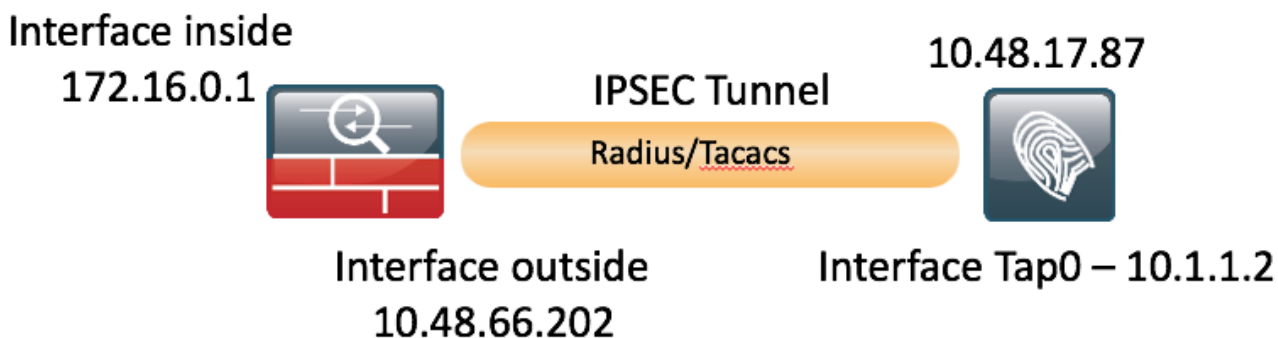
Общая Методика поиска и устранения проблем VPN может быть применена для решения проблем, отнесенных к IPSEC. Можно найти полезные документы ниже:

[Отладки IOS IKEv2 для сквозного VPN-соединение с техническими примечаниями по поиску и устранению проблем PSK](#)

[Отладки ASA IKEv2 для сквозного VPN-соединение с PSK](#)

Настройте от узла к узлу FlexVPN (DVTI к криптокарте) между NAD и ISE 2.2

Также возможно защитить Трафик сервера RADIUS с FlexVPN. Следующая топология используется в примере ниже:



Конфигурация FlexVPN является прямой. Больше подробных данных может быть найдено [здесь](#):

<http://www.cisco.com/c/en/us/support/docs/security/flexvpn/116008-flexvpn-nge-config-00.html>

Конфигурация ASA

```
crypto map MAP interface outside
```

Конфигурация ESR на ISE

```
crypto map MAP interface outside
```

Вопросы проектирования FlexVPN

- VPN-туннель создан с помощью DVTI на стороне ESR, и Криптокарта на стороне ASA, с конфигурацией выше ASA в состоянии генерировать Пакет RADIUS, инициируемый из внутреннего интерфейса, который гарантирует корректный access-list для шифрования для инициирования установления сеанса VPN.
- Обратите внимание, что в этом ASA случае NAD должен быть определен на ISE с IP-адресом внутреннего интерфейса.