Отладки ASA IKEv2 для устранения проблем VPN для удаленного доступа

Содержание

Введение

Этот документ описывает, как понять отладки на устройстве адаптивной защиты Cisco (ASA), когда вторая версия протокола Internet Key Exchange (IKEv2) используется с защищенным мобильным клиентом Cisco AnyConnect Secure Mobility. Этот документ также предоставляет сведения о том, как преобразовать определенные линии отладки в конфигурации ASA.

Этот документ не описывает, как передать трафик после того, как VPN-туннель был установлен к ASA, и при этом это не включает базовые понятия IPSec или IKE.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с обменом пакетами для IKEv2. Для получения дополнительной информации обратитесь к Отладке Обмена пакетами и Уровня протокола IKEv2.

Используемые компоненты

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

- Вторая версия протокола Internet Key Exchange (IKEv2)
- Устройство адаптивной защиты Cisco (ASA) Версия 8.4 или 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.

Базовая проблема

Центр технической поддержки Cisco (TAC) часто использует IKE и команды отладки IPSec для понимания, где существует проблема с установлением VPN-туннеля IPSec, но команды могут быть загадочными.

Сценарий

Команды "debug"

```
debug crypto ikev2 protocol 127
debug crypto ikev2 platform 127
debug aggregate-auth xml 5
```

Конфигурация ASA

Эта конфигурация ASA является строго основной без использования внешних серверов.

```
interface Ethernet0/1
 nameif outside
 security-level 0
 ip address 10.0.0.1 255.255.255.0

ip local pool webvpn1 10.2.2.1-10.2.2.10

crypto ipsec ikev2 ipsec-proposal 3des
 protocol esp encryption aes-256 aes 3des des
 protocol esp integrity sha-1
crypto dynamic-map dynmap 1000 set ikev2 ipsec-proposal 3des
crypto map crymap 10000 ipsec-isakmp dynamic dynmap
crypto map crymap interface outside

crypto ca trustpoint Anu-ikev2
 enrollment self
 crl configure

crypto ikev2 policy 10
 encryption aes-192
```

```
 integrity sha
 group 2
 prf sha
 lifetime seconds 86400

crypto ikev2 enable outside client-services port 443
crypto ikev2 remote-access trustpoint Anu-ikev2
ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1
ssl trust-point Anu-ikev2 outside

webvpn
 enable outside
 anyconnect image disk0:/anyconnect-win-3.0.1047-k9.pkg 1
 anyconnect profiles Anyconnect-ikev2 disk0:/anyconnect-ikev2.xml
 anyconnect enable
 tunnel-group-list enable

group-policy ASA-IKEV2 internal
group-policy ASA-IKEV2 attributes
 wins-server none
 dns-server none
 vpn-tunnel-protocol ikev2
 default-domain none
 webvpn
 anyconnect modules value dart
 anyconnect profiles value Anyconnect-ikev2 type user

username Anu password lAuoFgF7KmB3D0WI encrypted privilege 15

tunnel-group ASA-IKEV2 type remote-access
tunnel-group ASA-IKEV2 general-attributes
 address-pool webvpn1
 default-group-policy ASA-IKEV2
tunnel-group ASA-IKEV2 webvpn-attributes
 group-alias ASA-IKEV2 enable
```

XML-файл

```
<ServerList>
       <HostEntry>
               <HostName>Anu-IKEV2</HostName>
               <HostAddress>10.0.0.1</HostAddress>
               <UserGroup>ASA-IKEV2</UserGroup>
               <PrimaryProtocol>IPsec</PrimaryProtocol>
       </HostEntry>
</ServerList>
```

Примечание: Название UserGroup в профиле клиента XML должно совпасть с названием туннельной группы на ASA. В противном случае, сообщение об ошибках 'Недопустимая Запись хоста. Повторно введите', замечен на клиенте AnyConnect.

Журналы отладки и описания

Примечание: Журналы от Диагностики и средства создания отчетов (DART) обычно очень болтливы, таким образом, определенные журналы DART были опущены в данном примере из-за незначительности.

Описание сообщения сервера	Отладка	Опис сообщ
	Дата : 23.04.2013 Время : 16:24:55 Введите : Информация Источник: acvpnui Описание: Функция: ClientIfcBase:: подключение Файл:.\ClientIfcBase.cpp Линия: 964 **VPN-подключение к Anu-IKEV2 запросил пользователь.** ********** Дата : 23.04.2013 Время : 16:24:55 Введите : Информация Источник: acvpnui Описание: Информация о типе сообщения, передаваемая пользователю: Контакт Anu-IKEV2. ********** Дата : 23.04.2013 Время : 16:24:55 Введите : Информация Источник: acvpnui Описание: Функция: ApiCert:: getCertList Файл:.\ApiCert.cpp Линия: 259 Количество сертификатов нашло: 0 ********** Дата : 23.04.2013 Время : 16:25:00 Введите : Информация Источник: acvpnui Описание: **Инициирование VPN-подключения к защищенному шлюзу https://10.0.0.1/ASA-IKEV2** ********** Дата : 23.04.2013 Время : 16:25:00 Введите : Информация Источник: acvpnagent Описание: Туннель инициируется Графическим клиентом. ********** Дата : 23.04.2013 Время : 16:25:02 Введите : Информация Источник: acvpnagent Описание: Функция: CIPsecProtocol:: connectTransport	Клиен VPN-т

	Файл:.\IPsecProtocol.cpp Линия: 1629 **Открытый сокет IKE от 192.168.1.1:25170 до 10.0.0.1:500** ********** **----------Exchange IKE_SA_INIT запускает----------**
ASA получает сообщение IKE_SA_INIT от клиента.	IKEv2-PLAT-4: PKT RECV [IKE_SA_INIT] [192.168.1.1]:25170-> [10.0.0.1]:500 InitSPI=0x58aff71141ba436b RespSPI=0x0000000000000000 MID=00000000 IKEv2-PROTO-3: Rx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0] m_id: 0x0
Первая пара сообщений является обменом IKE_SA_INIT. Эти сообщения выполняют согласование о криптографических алгоритмах, обмениваются параметрами и делают обмен Diffie-Hellman (DH). Сообщение IKE_SA_INIT, полученное от клиента, содержит эти поля: 1. **Заголовок ISAKMP** - SPI/версия/флаги. 2. **SAi1** - Криптографический алгоритм тот инициатор IKE поддержки. 3. **KEi** - Значение открытого ключа DH инициатора. 4. **N -** Параметр инициатора.	IKEv2-PROTO-3: **HDR** [i:58AFF71141BA436B - r: 0000000000000000] IKEv2-PROTO-4: **IKEV2 HDR ispi: 58AFF71141BA436B - rspi: 0000000000000000** IKEv2-PROTO-4: Следующее информационное наполнение: SA, **версия: 2.0** IKEv2-PROTO-4: Тип Exchange: IKE_SA_INIT, **флаги: INITIATOR** IKEv2-PROTO-4: Идентификатор сообщения: 0x0, длина: 528 **SA** Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 168 IKEv2-PROTO-4: последнее предложение: 0x0, зарезервированный: 0x0, длина: 164 Предложение: 1, Идентификатор протокола: IKE, размер SPI: 0, #trans: 18 IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12 введите : 1, зарезервированный: 0x0, идентификатор: CBC AES IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12 введите : 1, зарезервированный: 0x0, идентификатор: CBC AES IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12 введите : 1, зарезервированный: 0x0, идентификатор: CBC AES IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8 введите : 1, зарезервированный: 0x0, идентификатор: 3DES IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8 введите : 1, зарезервированный: 0x0, идентификатор: DES IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8 введите : 2, зарезервированный: 0x0, идентификатор: SHA512 IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8 введите : 2, зарезервированный: 0x0, идентификатор: SHA384

IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA256
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: MD5
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA512
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA384
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA256
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: MD596
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1536_MODP/Group 5
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_1024_MODP/Group 2
IKEv2-PROTO-4 : последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_768_MODP/Group 1

KE Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 104
Группа DH: 1, Зарезервированный: 0x0

eb 5e 29 fe cb 2e d1 28 ed 4a 54 b1 13 7c b8 89
f7 62 13 6b df 95 88 28 b5 97 ba 52 ef e4 1d 28
ca 06 d1 36 b6 67 32 9a c2 dd 4e d8 c7 80 de 20
36 34 c5 b3 3e 1d 83 1a c7 fb 9d b8 c5 f5 ed 5f
ba ba 4f b6 b2 e2 2-e 43 4f a0 b6 90 9a 11 3f 7d
0a 21 c3 4d d3 0a d2 1e 33 43 d3 5e cc 4b 38 e0

N Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 24

20 12 8f 22 7b 16 23 52 e4 29 4d 98 c7 fd a8 77
ce 7c 0b b4
IKEv2-PROTO-5: Проанализируйте Определяемое поставщиком Информационное наполнение: VID СИСКО-ДЕЛЕТ-РИСОНА Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 23

ASA проверяет и обрабатывает Сообщение IKE_INIT. ASA:

1. Выбирает крипто-комплект из предлагаемые инициатором.
2. Вычисляет его собственный секретный ключ DH.
3. Вычисляет значение SKEYID из для которого могут быть получены все ключи этот IKE_SA. Заголовки всех последующие сообщения зашифрованный и аутентифицируемый. ключи, используемые для шифрования и защита целостности получена от SKEYID и известны как:

   SK_e - Шифрование.**SK_a** - Authentication.**SK_d** - Полученный и используемый для деривации далее материал для кодирования для CHILD_SAs.Отдельный SK_e и SK_a вычисленный для каждого направления.

Дешифрованный packet:Data: 528 байтов
IKEv2-PLAT-3: Обработайте пользовательские информационные наполнения VID
IKEv2-PLAT-3: VID Авторского права Cisco получен от узла
IKEv2-PLAT-3: VID EAP AnyConnect получен от узла
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: **EV_RECV_INIT**
IKEv2-PROTO-3: (6): Проверьте обнаружение NAT
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): проверка Перенаправления не необходима, пропуская его
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK_CAC
IKEv2-PLAT-5: **Новый запрос ikev2 sa признал**
IKEv2-PLAT-5: Приращение поступления, выполняющего согласование sa, рассчитывает одним
IKEv2-PLAT-5: НЕДОПУСТИМЫЙ МАРКЕР PSH
IKEv2-PLAT-5: НЕДОПУСТИМЫЙ МАРКЕР PSH
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK_COOKIE
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: IDLE Event: EV_CHK4_COOKIE_NOTIFY
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Событие R_INIT: **EV_VERIFY_MSG**
IKEv2-PROTO-3: (6): **сообщение Init Verify SA**
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Событие R_INIT: EV_INSERT_SA
IKEv2-PROTO-3: (6): Insert SA
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Событие R_INIT: EV_GET_IKE_POLICY
IKEv2-PROTO-3: (6): **Получение настроенной политики**
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000000 CurState: Событие R_INIT: **EV_PROC_MSG**
IKEv2-PROTO-2: (6): Обрабатывание начального сообщения

Соответствующая конфигурация:

```
crypto ikev2 policy 10
 encryption aes-192 integrity
sha group 2  prf sha lifetime
seconds 86400
crypto ikev2 enable outside
```

IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_INIT: EV_DETECT_NAT
IKEv2-PROTO-3: (6): обнаружение NAT Процесса уведомляет
IKEv2-PROTO-5: (6): Обработка nat обнаруживает src,
уведомляют
IKEv2-PROTO-5: (6): Удаленный адрес, с которым не
совпадают
IKEv2-PROTO-5: (6): Обработка nat обнаруживает dst,
уведомляют
IKEv2-PROTO-5: (6): Локальный адрес совпал
IKEv2-PROTO-5: (6): Хостом является расположенный NAT
снаружи
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_INIT:
EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Полученные допустимые данные режима
конфигурации
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_INIT:
EV_SET_RECD_CONFIG_MODE
IKEv2-PROTO-3: (6): Установите полученные данные режима
конфигурации
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_SET_POLICY
IKEv2-PROTO-3: (6): **Установка настроенной политики**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_CHK_AUTH4PKI
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_PKI_SESH_OPEN
IKEv2-PROTO-3: (6): Открытие сеанса PKI
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_GEN_DH_KEY
IKEv2-PROTO-3: (6): **Вычислительный открытый ключ DH**
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_NO_EVENT
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_OK_RECD_DH_PUBKEY_RESP

IKEv2-PROTO-5: (6): Действие: Action_Null
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_GEN_DH_SECRET
IKEv2-PROTO-3: (6): **Вычислительный секретный ключ DH**
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_NO_EVENT
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_OK_RECD_DH_SECRET_RESP
IKEv2-PROTO-5: (6): Действие: Action_Null
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_GEN_SKEYID
IKEv2-PROTO-3: (6): **Генерируйте skeyid**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_GET_CONFIG_MODE
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000000 CurState: Событие R_BLD_INIT:
EV_BLD_MSG
IKEv2-PROTO-2: (6): **Передача начального сообщения**
IKEv2-PROTO-3: Предложение ike: 1, размер SPI: 0
(начальное согласование),
Цифра. преобразовывает: 4
CBC AES SHA1 SHA96 DH_GROUP_768_MODP/Group 1
IKEv2-PROTO-5: Создайте Определяемое поставщиком
Информационное наполнение: DELETE-REASONIKEv2-
PROTO-5: Создайте Определяемое поставщиком
Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) IKEv2-
PROTO-5: Создайте Определяемое поставщиком
Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) IKEv2-
PROTO-5: Конструкция Уведомляет Информационное
наполнение: NAT_DETECTION_SOURCE_IPIKEv2-PROTO-5:
Конструкция Уведомляет Информационное наполнение:
NAT_DETECTION_DESTINATION_IPIKEv2-PLAT-2:
Подведенный для получения хэшей отправителей, которым
доверяют, или ни одного доступного
IKEv2-PROTO-5: Создайте Определяемое поставщиком
Информационное наполнение: FRAGMENTATIONIKEv2-
PROTO-3: Tx [L 10.0.0.1:500/R 192.168.1.1:25170/VRF i0:f0]
m_id: 0x0
IKEv2-PROTO-3: **HDR** [i:58AFF71141BA436B - r:
FC696330E6B94D7F]
IKEv2-PROTO-4: **IKEV2 HDR ispi: 58AFF71141BA436B - rspi:**

ASA создает ответное сообщение для обмена IKE_SA_INIT.
Этот пакет содержит:

1. **Заголовок ISAKMP** - SPI/версия/флаги.
2. **SAr1** - Криптографический алгоритм, который выбирает респондент IKE.
3. **KEr** - Значение открытого ключа DH респондента.
4. **N -** Параметр респондента.

FC696330E6B94D7F
IKEv2-PROTO-4: Следующее информационное наполнение: SA, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_SA_INIT, **флаги: ОТВЕТ MSG РЕСПОНДЕНТА**
IKEv2-PROTO-4: Идентификатор сообщения: 0x0, длина: 386
SA Следующее информационное наполнение: KE, зарезервированный: 0x0, длина: 48
IKEv2-PROTO-4: последнее предложение: 0x0, зарезервированный: 0x0, длина: 44
Предложение: 1, Идентификатор протокола: IKE, размер SPI: 0, #trans: 4
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 2, зарезервированный: 0x0, идентификатор: SHA1
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
IKEv2-PROTO-4 : последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 4, зарезервированный: 0x0, идентификатор: DH_GROUP_768_MODP/Group 1

KE Следующее информационное наполнение: N, зарезервированный: 0x0, длина: 104
Группа DH: 1, Зарезервированный: 0x0

c9 30 f9 32 d4 7c d1 a7 5b 71 72 09 6e 7e 91 0c
e1 ce b4 a4 3c f2 8b 74 4e 20 59 b4 0b a1 и следующие 65
37 88 cc c4 a4 b6 fa 4a 63 03 93 89 e1 7e bd 6a
64 9a 38 24 e2 a8 40 f5 a3 d6 ef f7 1a df 33 cc
система цифрового управления a1 8e fa 9c 34 45 79 1a 7c 29 05 87 8a ac 02
98 2e 7d cb 41 51 d6 fe fc c7 76 83 1d 03 b0 d7
N Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 24

c2 28 7f 8c 7d b3 1e 51 fc eb f1 97 ec 97 b8 67
d5 e7 c2 f5
VID Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 23

ASA отсылает ответное сообщение для обмена IKE_SA_INIT. Обмен IKE_SA_INIT теперь завершен. ASA запускает таймер для процесса проверки подлинности.

IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_SA_INIT] [10.0.0.1]:500-> [192.168.1.1]:25170 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000000
IKEv2-PROTO-5: (6):

********** Дата : 23.04.2013 Время : 16:25:02 Введите : Информация Источник: acvpnagent Описание: Функция: CIPsecProtocol:: initiateTunnel

Клиен Тунне 'иници

Трассировка SM-> SA:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F
(R) MsgID = 00000000
CurState: Событие
INIT_DONE: EV_DONE
IKEv2-PROTO-3: (6):
Фрагментация включена
IKEv2-PROTO-3: (6): Cisco
DeleteReason Уведомляет,
включен
IKEv2-PROTO-3: (6): обмен
Init Complete SA
IKEv2-PROTO-5: (6):
Трассировка SM-> SA:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F
(R) MsgID = 00000000
CurState: Событие
INIT_DONE: EV_CHK4_ROLE
IKEv2-PROTO-5: (6):
Трассировка SM-> SA:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F
(R) MsgID = 00000000
CurState: Событие
INIT_DONE: EV_START_TMR
IKEv2-PROTO-3: (6):
Стартовый таймер для
ожидания сообщения
аутентификации (30 сек.)
IKEv2-PROTO-5: (6):
Трассировка SM-> SA:
I_SPI=58AFF71141BA436B
R_SPI=FC696330E6B94D7F
(R) MsgID = 00000000
CurState: Событие
R_WAIT_AUTH:
EV_NO_EVENT

Файл:.\IPsecProtocol.cpp
Линия: 345
Туннель IPSec инициирует
****

----------IKE_SA_INIT Завершенный----------

----------IKE_AUTH начинает----------

****

Дата : 23.04.2013
Время : 16:25:00
Введите : Информация
Источник: acvpnagent

Описание: Параметры защищенного шлюза:
IP-адрес: 10.0.0.1
Порт: 443
Url : "10.0.0.1"

Клиен
инфор
напол
из сос
указан
желан
испол
расши
прове
подли

Подлинный метод: **IKE - AnyConnect EAP**
Идентичность IKE:
****
Дата : 23.04.2013
Время : 16:25:00
Введите : Информация
Источник: acvpnagent

Описание: **Инициируя соединение защищенного мобильного клиента Cisco AnyConnect Secure Mobility, версию 3.0.1047**
****
Дата : 23.04.2013
Время : 16:25:02
Введите : Информация
Источник: acvpnagent

Описание: Функция: ikev2_log
Файл:.\ikev2_anyconnect_osal.cpp
Линия: 2730
Полученный запрос установить Туннель IPSec; селектор локального трафика = Диапазон адресов: 0.0.0.0-255.255.255.255 Протокол: 0 Диапазонов портов: 0-65535; удаленный селектор трафика = Диапазон адресов: 0.0.0.0-255.255.255.255 Протокол: 0 Диапазонов портов: 0-65535
****
Дата : 23.04.2013
Время : 16:25:02
Введите : Информация
Источник: acvpnagent

Описание: Функция: CIPsecProtocol:: connectTransport
Файл:.\IPsecProtocol.cpp
Линия: 1629
Открытый сокет IKE от 192.168.1.1:25171 до 10.0.0.1:4500
****

Аутентификация сделана с EAP. Только одиночный метод аутентификации EAP позволен в рамках диалога EAP. ASA получает сообщение IKE_AUTH от клиента.

IKEv2-PLAT-4: **PKT RECV [IKE_AUTH]** [192.168.1.1]:25171-> **[10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000001**
IKEv2-PROTO-3: **Rx** [L 10.0.0.1:4500/R 192.168.1.1:25171/VRFi0:f0] m_id: 0x1

Когда клиент включает информационное наполнение IDI но не информационное наполнение AUTH, указывает это клиент объявил идентичность, но имеет не доказанный это. В отладках, AUTH информационное

IKEv2-PROTO-3: **HDR** [i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F**
IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, **версия: 2.0**
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, **флаги: INITIATOR**
IKEv2-PROTO-4: Идентификатор сообщения: 0x1, длина: 540
IKEv2-PROTO-5: (6): Запрос имеет mess_id 1; ожидаемый 1 до 1
РЕАЛЬНЫЙ Дешифрованный packet:Data: 465 байтов

аутен
Прото
задае
подра
клиен
профи
профи
содер
<IKEI
перед
инфор
напол
ID_GR
неподд
строк
$AnyC
Клиен
соеди
на пор

наполнение не присутствует в IKE_AUTH
пакет передан клиентом. Клиент
передает информационное наполнение AUTH только после
Обмен EAP успешен. Если ASA
готово использовать расширяемое
метод аутентификации, это размещает EAP информационное наполнение в сообщении 4 и отсрочивает передачу SAr2, TSI и TSr до инициатора
аутентификация завершена в а
последующий обмен IKE_AUTH.
Пакет инициатора IKE_AUTH содержит:

1. **Заголовок ISAKMP** - SPI/версия/флаги.
2. **IDI** - имя группы туннелей это клиент хочет соединиться с может быть отправлен IDI информационное наполнение вводит ID_KEY_ID начальное сообщение Обмен IKE_AUTH. Это когда клиентский профиль*, происходит предварительно сконфигурированный с именем группы или, после предыдущего успешного аутентификация, клиент имеет кэшируемый имя группы в привилегированный

IKEv2-PROTO-5: Проанализируйте Определяемое поставщиком Информационное наполнение: (ПОЛЬЗОВАТЕЛЬСКИЙ) VID Следующее информационное наполнение: IDI, зарезервированный: 0x0, длина: 20

f6 11 52 8d b0 2c b8 da 30 46 на 58 акрофутов быть 91 56 fa
IDI Следующее информационное наполнение: CERTREQ, зарезервированный: 0x0, длина: 28
ID Type: Имя группы, Зарезервированное: 0x0 0x0

2a 24 41 6e 79 43 6f 6e 6e 65 63 74 43 6c 69 65
6e 74 24 2a
CERTREQ Следующее информационное наполнение: CFG, зарезервированный: 0x0, длина: 25
Свидетельство, кодирующее Сертификат X.509 - подпись CertReq data: 20 байтов
CFG Следующее информационное наполнение: SA, зарезервированный: 0x0, длина: 196
тип cfg: **CFG_REQUEST**, зарезервированный: 0x0, зарезервированный: 0x0

тип attrib: внутренний адрес IP4, длина: 0

тип attrib: внутренняя маска подсети IP4, длина: 0

тип attrib: внутренний IP4 DNS, длина: 0

тип attrib: внутренний IP4 NBNS, длина: 0

тип attrib: истечение внутреннего адреса, длина: 0

тип attrib: версия приложения, длина: 27

41 6e 79 43 6f 6e 6e 65 63 74 20 57 69 6e 64 6f
77 73 20 33 2e 30 2e 31 30 34 37
тип attrib: внутренний адрес IP6, длина: 0

тип attrib: внутренняя подсеть IP4, длина: 0

тип attrib: Неизвестный - 28682, длина: 15

77 69 6e 78 70 36 34 74 65 6d 70 6c 61 74 65
тип attrib: Неизвестный - 28704, длина: 0

тип attrib: Неизвестный - 28705, длина: 0

тип attrib: Неизвестный - 28706, длина: 0

тип attrib: Неизвестный - 28707, длина: 0

тип attrib: Неизвестный - 28708, длина: 0

тип attrib: Неизвестный - 28709, длина: 0

файл. ASA
пытается совпасть с
туннельной группой
название с
содержанием IKE
Информационное
наполнение IDI. После
первого
успешный IPSEC VPN
установленный, кэши
клиента
имя группы то
(псевдоним группы), к
который
пользователь
аутентифицировался.
Эта группа
название отправлено в
IDI
информационное
наполнение
следующего
соединения
попытайтесь для
указания
вероятная группа,
желаемая
пользователь. Когда
Аутентификация eap
заданный или
подразумеваемый
клиентом
профиль и профиль не
делают
содержите
<IKEIdentity>
элемент, клиент
передает
ID_GROUP вводят
информационное
наполнение IDI
с неподвижной строкой
* $AnyConnectClient$*.

тип attrib: Неизвестный - 28710, длина: 0

тип attrib: Неизвестный - 28672, длина: 0

тип attrib: Неизвестный - 28684, длина: 0

тип attrib: Неизвестный - 28711, длина: 2

05 7e

тип attrib: Неизвестный - 28674, длина: 0

тип attrib: Неизвестный - 28712, длина: 0

тип attrib: Неизвестный - 28675, длина: 0

тип attrib: Неизвестный - 28679, длина: 0

тип attrib: Неизвестный - 28683, длина: 0

тип attrib: Неизвестный - 28717, длина: 0

тип attrib: Неизвестный - 28718, длина: 0

тип attrib: Неизвестный - 28719, длина: 0

тип attrib: Неизвестный - 28720, длина: 0

тип attrib: Неизвестный - 28721, длина: 0

тип attrib: Неизвестный - 28722, длина: 0

тип attrib: Неизвестный - 28723, длина: 0

тип attrib: Неизвестный - 28724, длина: 0

тип attrib: Неизвестный - 28725, длина: 0

тип attrib: Неизвестный - 28726, длина: 0

тип attrib: Неизвестный - 28727, длина: 0

тип attrib: Неизвестный - 28729, длина: 0

3. CERTREQ - Клиент запрос ASA для а предпочтительный сертификат.

SA Следующее информационное наполнение: TSI, зарезервированный: 0x0, длина: 124
IKEv2-PROTO-4: последнее предложение: 0x0, зарезервированный: 0x0, длина: 120
Предложение: 1, Идентификатор протокола: ESP, размер SPI: 4, #trans: 12
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC

Сертификат информационные наполнения запроса могут быть включены в обмене, когда отправитель потребности получить сертификат получатель. Запрос сертификата информационное наполнение обработано контроль 'Кодирования свидетельства' поле для определения имеет ли процессор кого-либо сертификаты этого типа. Если так, Поле 'Certification Authority' осмотренный, чтобы определить если процессор имеет любые сертификаты это может быть проверено до одного из указанная сертификация полномочия. Это может быть цепочкой сертификаты.

4. **CFG** - CFG_REQUEST/ CFG_REPLY позволяет IKE оконечная точка, чтобы запросить информацию от его узла. Если атрибут в Конфигурация CFG_REQUEST информационное наполнение не является нулевой длиной, это взятый в качестве

AES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC
AES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC
AES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: 3DES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: DES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 1, зарезервированный: 0x0, идентификатор: NULL
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA512
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA384
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA256
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: MD596
IKEv2-PROTO-4 : последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 5, зарезервированный: 0x0, идентификатор:

TSI Следующее информационное наполнение: TSr, зарезервированный: 0x0, длина: 24
Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16
начальный порт: 0, оконечный порт: 65535
запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255
TSr Следующее информационное наполнение: NOTIFY, зарезервированный: 0x0, длина: 24
Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор:

предложения для этого атрибут. CFG_REPLY информационное наполнение конфигурации может возвратиться то значение или новое. Это может также добавьте новые атрибуты и нет включайте некоторые запрошенные. Просители игнорируют, возвратился атрибуты, которые они не делают распознать. В этих отладках, клиент запрашивает туннель конфигурация в CFG_REQUEST. ASA отвечает на это и передает туннель атрибуты конфигурации только после обмен EAP успешен.

5. SAi2 - SAi2 инициирует SA, который подобен фазе 2 обмен набора преобразований в IKEv1.
6. TSI и TSr - инициатор и селекторы трафика респондента содержите, соответственно, источник и адрес назначения (DA) инициатор и респондент, чтобы к передайте и получите зашифрованный

0, длина: 16
начальный порт: 0, оконечный порт: 65535
запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255

	трафик. Диапазон адресов указывает что весь трафик к и от тот диапазон туннелирован. Если предложение приемлемо для респондент, это передает идентичный TS информационные наполнения назад.

Атрибуты клиент должны поставить для групповая аутентификация сохранена в Файл конфигурации AnyConnect. ***Соответствующая настройка профиля:**
`<ServerList>`
`<HostEntry>`
`<HostName>Anu-IKEV2 </HostName>`
`<HostAddress>10.0.0.1 </HostAddress>`
`<UserGroup>ASA-IKEV2 </UserGroup>`
`<PrimaryProtocol>IPsec </PrimaryProtocol>`
`</HostEntry>`
`</ServerList>`	

ASA генерирует ответ на сообщение IKE_AUTH и готовится аутентифицировать себя на клиенте.	**Дешифрованный packet:Data&colon**; 540 байтов IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_RECV_AUTH IKEv2-PROTO-3: (6): Остановка таймера для ожидания сообщения аутентификации IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_CHK_NAT_T IKEv2-PROTO-3: (6): Проверьте обнаружение NAT IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000001 CurState: Событие R_WAIT_AUTH: EV_CHG_NAT_T_PORT IKEv2-PROTO-2: (6): NAT обнаружил плавание к порту 25171 Init, resp порт 4500 IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)

MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_PROC_ID
IKEv2-PROTO-2: (6): Recieved допустимые параметры в
идентификаторе процесса
IKEv2-PLAT-3: (6) одноранговый подлинный набор метода к: 0
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_CHK_IF_PEER_CERT_NEEDS_TO_BE_FETCHED_FOR_PR
OF_SEL
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_GET_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Получение настроенной политики
IKEv2-PLAT-3: Новое Клиентское соединение AnyConnect,
обнаруженное на основе информационного наполнения ID
IKEv2-PLAT-3: my_auth_method = 1
IKEv2-PLAT-3: (6) одноранговый подлинный набор метода к:
256
IKEv2-PLAT-3: supported_peers_auth_method = 16
IKEv2-PLAT-3: (6) набор tp_name к: Anu-ikev2
IKEv2-PLAT-3: **доверяйте набору точки к:** Anu-ikev2
IKEv2-PLAT-3: ID P1 = 0
IKEv2-PLAT-3: перевод IKE_ID_AUTO к = 9
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_SET_POLICY
IKEv2-PROTO-3: (6): **Установка настроенной политики**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_VERIFY_POLICY_BY_PEERID
IKEv2-PROTO-3: (6): Проверьте политику узла
IKEv2-PROTO-3: (6): **Соответствующий сертификат найден**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_CHK_CONFIG_MODE
IKEv2-PROTO-3: (6): Полученные допустимые данные режима
конфигурации
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_SET_RECD_CONFIG_MODE
IKEv2-PLAT-3: (6) имя хоста DHCP для DDNS установлено в:
winxp64template
IKEv2-PROTO-3: (6): Установите полученные данные режима
конфигурации
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:

EV_CHK_AUTH4EAP
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_WAIT_AUTH:
EV_CHK_EAP
IKEv2-PROTO-3: (6): **Проверьте для обмена EAP**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие **R_BLD_AUTH**:
EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Генерируйте мои данные проверки подлинности**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_AUTH:
EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Получите мой метод аутентификации
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_AUTH: EV_SIGN
IKEv2-PROTO-3: (6): **Подпишите подлинные данные**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_AUTH:
EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_EAP_AUTH_REQ:
EV_AUTHEN_REQ
IKEv2-PROTO-2: (6): **То, чтобы просить, чтобы средство проверки подлинности отправило запрос EAP**
Созданная **стоимость аутентификации config** имени элемента
Добавленный клиент названия атрибута оценивает vpn к аутентификации config элемента
Добавленный тип названия атрибута оценивает привет к аутентификации config элемента
Созданная стоимость версии имени элемента 9.0 (2) 8
Добавленная версия имени элемента оценивает 9.0 (2) 8 к аутентификации config элемента
Добавленное название атрибута, кто оценивает sg к версии элемента
Генерируемое сообщение XML ниже
<? версия xml = "1.0" кодирование = "UTF 8"?>
<подлинный config клиент = "vpn" **вводит = "привет">**
<версия, кто = "sg"> 9.0 (2) 8 </версия>
</config-auth>

IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_EAP_AUTH_REQ:
EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Действие: Action_Null
IKEv2-PROTO-5: (6): Трассировка SM-> SA:

I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_EAP_AUTH_REQ: EV_CHK_REDIRECT
IKEv2-PROTO-3: (6): Перенаправление сверяется с платформой для распределения нагрузки
IKEv2-PLAT-3: Перенаправление проверяет платформу
IKEv2-PLAT-3: ikev2_osal_redirect: Сеанс принят 10.0.0.1
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000001 CurState: Событие R_BLD_EAP_AUTH_REQ: EV_SEND_EAP_AUTH_REQ
IKEv2-PROTO-2: (6): **Отправление запроса EAP**
IKEv2-PROTO-5: создайте определяемое поставщиком информационное наполнение: CISCO-GRANITEIKEv2-PROTO-3: (6): сборка

ASA передает информационное наполнение AUTH для запроса учетных данных пользователя от клиента.

IDr Следующее информационное наполнение: CERT, зарезервированный: 0x0, длина: 36
ID Type: DN ASN1 DER, зарезервированный: 0x0 0x0

30 1a 31 18 30 16 06 09 2a 86 48 86 f7 0d 01 09
02 16 09 41 53 41 2-й 49 4b 45 56 32

ASA передает метод AUTH как 'RSA', таким образом, это передает свой собственный сертификат клиенту, таким образом, клиент может аутентифицировать сервер ASA.

CERT Следующее информационное наполнение: CERT, зарезервированный: 0x0, длина: 436
Свидетельство, кодирующее Сертификат **X.509** - подпись Свидетельство data: 431 байт

Так как ASA готов использовать метод расширенной проверки подлинности, он размещает информационное наполнение EAP в сообщение 4 и отсрочивает передачу SAr2, TSI и TSr, пока аутентификация инициатора не завершена в последующем обмене IKE_AUTH. Таким образом те три информационных наполнения не присутствуют в отладках.

CERT Следующее информационное наполнение: AUTH, зарезервированный: 0x0, длина: 436
Свидетельство, кодирующее Сертификат X.509 - подпись Свидетельство data: 431 байт

AUTH Следующее информационное наполнение: EAP, зарезервированный: 0x0, длина: 136
Подлинный RSA метода, зарезервированный: 0x0, зарезервированный 0x0
Аутентификация data: 128 байтов

EAP Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 154
Код: запрос: **идентификатор**: 1, **длина**: 150
Введите : Неизвестный - 254
Данные EAP: 145 байтов

Пакет EAP содержит:

1. **Код: запрос** - Этот код передается средством проверки подлинности узлу.
2. **идентификатор: 1** - идентификатор помогает совпадать с ответами EAP с

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x1
IKEv2-PROTO-3: **HDR** [i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: **IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F**
IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, **флаги: ОТВЕТ MSG РЕСПОНДЕНТА**
IKEv2-PROTO-4: Идентификатор сообщения: 0x1, длина: 1292
ENCR Следующее информационное наполнение: VID, зарезервированный: 0x0, длина: 1264

запросами. Здесь значение равняется 1, который указывает, что это - первый пакет в обмене EAP. Этот запрос EAP имеет 'подлинный config' тип 'привет'; это передается от ASA до клиента для инициирования обмена EAP.

3. **Длина: 150** - Длина пакета EAP включает код, идентификатор, длину и данные EAP.
4. **Данные EAP**.

```
Зашифрованный data&colon; 1260 байтов
```

Фрагментация может закончиться, если сертификаты являются большими или если включены цепочки сертификатов. И информационные наполнения KE инициатора и респондента могут также включать большие ключи, которые могут также способствовать фрагментации.

```
IKEv2-PROTO-5: (6): Фрагментируя пакет, MTU Фрагмента:
544, Количество фрагментов: 3, ID Фрагмента: 1
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000001
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000001
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000001
```

```
****************************************
Дата       : 23.04.2013
Время       : 16:25:02
       Введите : Информация
     Источник: acvpnagent

Описание: Функция: ikev2_verify_X509_SIG_certs
Файл:.\ikev2_anyconnect_osal.cpp
Линия: 2077
Запрос принятия сертификата от пользователя
****************************************
Дата       : 23.04.2013
Время       : 16:25:02
       Введите : Ошибка
     Источник: acvpnui

Описание: Функция: CCapiCertificate:: verifyChainPolicy
Файл:.\Certificates\CapiCertificate.cpp
Линия: 2032
Вызванная функция: CertVerifyCertificateChainPolicy
```

Серти
перед
предо
польз
Серти
недов
EAP я
ANYC

Код возврата:-2146762487 (0x800B0109)
Описание: Цепочка сертификатов обработала, но завершенный в корневом сертификате, которому не доверяет трастовый поставщик.
****

Дата : 23.04.2013
Время : 16:25:04
Введите : Информация
Источник: acvpnagent

Описание: Функция: CEAPMgr:: dataRequestCB
Файл:.\EAPMgr.cpp
Линия: 400
EAP предложил тип: ANYCONNECT EAP
****

Клиент отвечает на запрос EAP с ответом.
Пакет EAP содержит:

1. **Код: ответ** - Этот код передается узлом средству проверки подлинности в ответ на запрос EAP.
2. **идентификатор: 1 -** идентификатор помогает совпадать с ответами EAP с запросами. Здесь значение равняется 1, который указывает, что это - ответ на запрос, ранее отправленный ASA (средство проверки подлинности). Этот ответ EAP имеет 'подлинный config' тип 'Init'; клиент инициализирует обмен EAP и ждет ASA для генерации запроса аутентификации.
3. **Длина: 252** - Длина пакета EAP включает код, идентификатор, длину и данные EAP.
4. **Данные EAP**.

ASA дешифрует этот ответ, и клиент говорит, что это получило информационное наполнение AUTH в

IKEv2-PLAT-4: **PKT RECV [IKE_AUTH]** [192.168.1.1]:25171-> [10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002
IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRFi0:f0] m_id: 0x2
IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, флаги: INITIATOR
IKEv2-PROTO-4: Идентификатор сообщения: 0x2, длина: 332
IKEv2-PROTO-5: (6): Запрос имеет mess_id 2; ожидаемый 2 до 2
РЕАЛЬНЫЙ Дешифрованный packet:Data: 256 байтов
EAP Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 256
Код: ответ: идентификатор: 1, **длина**: 252
Введите : Неизвестный - 254
EAP data:247 байты
Дешифрованный packet:Data&colon; 332 байта
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_WAIT_EAP_RESP: EV_RECV_AUTH
IKEv2-PROTO-3: (6): Остановка таймера для ожидания сообщения аутентификации
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Обработка ответа EAP**
Полученное сообщение XML ниже от клиента

предыдущем пакете (с сертификатом) и получило первый пакет запроса EAP от ASA. Это - то, что содержит ответный пакет EAP 'Init'.

<? версия xml = "1.0" кодирование = "UTF 8"?>
<подлинный config клиент = "vpn" **вводит = "Init"**>
<device-id> победа </device-id>
<версия, кто = "vpn"> 3.0.1047 </версия>
<выберите группа> ASA-IKEV2 </group-select>
<групповой доступ> ASA-IKEV2 </group-access>
</config-auth>
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_PROC_EAP_RESP: **EV_RECV_EAP_AUTH**
IKEv2-PROTO-5: (6): Действие: Action_Null
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_BLD_EAP_REQ: **EV_RECV_EAP_REQ**

Это - второй запрос, отправленный ASA клиенту. Пакет EAP содержит:

1. **Код: запрос** - Этот код передается средством проверки подлинности узлу.
2. **идентификатор: 2** - идентификатор помогает совпадать с ответами EAP с запросами. Здесь значение равняется 2, который указывает, что это - второй пакет в обмене. Этот запрос имеет 'подлинный config' тип 'запроса на аутентификацию'; ASA запрашивает что клиентская передача учетные данные проверки подлинности пользователя.
3. **Длина: 457** - Длина пакета EAP включает код, идентификатор, длину и данные EAP.
4. **Данные EAP**.

Информационное наполнение **ENCR**:
Это информационное наполнение дешифровано, и его содержание

IKEv2-PROTO-2: (6): Отправление запроса EAP **Генерируемое сообщение XML ниже**
<? версия xml = "1.0" кодирование = "UTF 8"?>
<подлинный config клиент = "vpn" **вводит = "запрос на аутентификацию"**>
<версия, кто = "sg"> 9.0 (2) 8 </версия>
<непрозрачный - для = "sg">
<туннельная группа> ASA-IKEV2 </tunnel-group>
<хэш config> 1367268141499 </config-hash>
</непрозрачный>
<csport> 443 </csport>
<подлинный идентификатор = "основной">
<форма>
<вводят тип = "текстовое" название = метка "имени пользователя" = "Имя пользователя":> </input>
<вводят тип = название "пароля" = метка "пароля" = "Пароль":> </input>
</форма>
</аутентификация>
</config-auth>
IKEv2-PROTO-3: (6): Построение пакета для шифрования; содержание:
EAP Следующее информационное наполнение: NONE,

********** Прове
Дата : 23.04.2013 подли
Время : 16:25:04 польз
Введите : Информация запро
Источник: acvpnui перед
как от
Описание: Функция: следу
SDIMgr:: ProcessPromptData ('подл
Файл:.\SDIMgr.cpp
Линия: 281
Тип проверки подлинности не является SDI.
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnui

Описание: Функция: ConnectMgr:: userResponse
Файл:.\ConnectMgr.cpp
Линия: 985
Обработка отклика пользователя.
****

проанализировано как дополнительные информационные наполнения.

зарезервированный: 0x0, длина: 461
Код: запрос: идентификатор: 2, длина: 457
Введите : Неизвестный - 254
Данные EAP: 452 байта

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x2
IKEv2-PROTO-3: **HDR** [i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, флаги: **ОТВЕТ MSG РЕСПОНДЕНТА**
IKEv2-PROTO-4: Идентификатор сообщения: 0x2, длина: 524
ENCR Следующее информационное наполнение: EAP, зарезервированный: 0x0, длина: 496
Зашифрованный data: 492 байта

IKEv2-PLAT-4: **ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]** [10.0.0.1]:4500-> [192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000002
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_BLD_EAP_REQ: EV_START_TMR
IKEv2-PROTO-3: (6):

	Стартовый таймер для ожидания пользовательского сообщения аутентификации (120 сек.) IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000002 CurState: Событие R_WAIT_EAP_RESP: EV_NO_EVENT
Клиент передает другое сообщение инициатора IKE_AUTH с информационным наполнением EAP. Пакет EAP содержит: 1. **Код: ответ** - Этот код передается узлом средству проверки подлинности в ответ на запрос EAP. 2. **идентификатор: 2** - идентификатор помогает совпадать с ответами EAP с запросами. Здесь значение равняется 2, который указывает, что это - ответ на запрос, ранее отправленный ASA (средство проверки подлинности). 3. **Длина: 420** - Длина пакета EAP включает код, идентификатор, длину и данные EAP. 4. **Данные EAP**.	IKEv2-PLAT-4: PKT RECV [IKE_AUTH] [192.168.1.1]:25171-> [10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000003 IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x3 IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r: FC696330E6B94D7F] IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0 IKEv2-PROTO-4: **Тип Exchange: IKE_AUTH, флаги: INITIATOR** IKEv2-PROTO-4: Идентификатор сообщения: 0x3, длина: 492 IKEv2-PROTO-5: (6): Запрос имеет mess_id 3; ожидаемый 3 до 3 РЕАЛЬНЫЙ Дешифрованный packet:Data: 424 байта **EAP** Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 424 **Код: ответ: идентификатор: 2**, длина: 420 Введите : Неизвестный - 254 **Данные EAP**: 415 байтов
ASA обрабатывает этот ответ. Клиент запросил, чтобы пользователь ввел учетные данные. Этот ответ EAP имеет 'подлинный config' тип 'подлинного ответа'. Этот пакет содержит учетные данные, введенные пользователем.	Дешифрованный packet:Data: 492 байта IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Событие R_WAIT_EAP_RESP: EV_RECV_AUTH IKEv2-PROTO-3: (6): Остановка таймера для ожидания сообщения аутентификации IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000003 CurState: Событие R_WAIT_EAP_RESP: EV_RECV_EAP_RESP IKEv2-PROTO-5: (6): Трассировка SM-> SA:

I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000003 CurState: Событие R_PROC_EAP_RESP:
EV_PROC_MSG
IKEv2-PROTO-2: (6): **Обработка ответа EAP**
Полученное сообщение XML ниже от клиента
<? версия xml = "1.0" кодирование = "UTF 8"?>
<подлинный config клиент = "vpn" **вводит = "подлинный ответ"**>
<device-id> победа </device-id>
<версия, кто = "vpn"> 3.0.1047 </версия>
<маркер сеанса> </session-token>
<идентификатор сеанса> </session-id>
<непрозрачный - для = "sg">
<туннельная группа> **ASA-IKEV2** </tunnel-group>
<хэш config> 1367268141499 </config-hash> </непрозрачный>
<аутентификация>
<password> cisco123 </пароль>
<Username> Anu </имя пользователя> </аутентификация>
</config-auth>
IKEv2-PLAT-1: **проверка подлинности пользователя**
EAP:Initiated
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000003 CurState: Событие R_PROC_EAP_RESP:
EV_NO_EVENT
IKEv2-PLAT-5: обратный вызов AAA EAP:In
Полученный дайджест свидетельства сервера:
DACE1C274785F28BA11D64453096BAE294A3172E
IKEv2-PLAT-5: **EAP:success в обратном вызове AAA**
IKEv2-PROTO-3: Полученный ответ от средства проверки подлинности
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000003 CurState: Событие R_PROC_EAP_RESP:
EV_RECV_EAP_AUTH
IKEv2-PROTO-5: (6): Действие: Action_Null
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000003 CurState: Событие R_BLD_EAP_REQ:
EV_RECV_EAP_REQ
IKEv2-PROTO-2: (6): Отправление запроса EAP
Генерируемое сообщение XML ниже
<? версия xml = "1.0" кодирование = "UTF 8"?>
<подлинный config клиент = "vpn" **вводит = "завершенный"**>
<версия, кто = "sg"> 9.0 (2) 8 </версия>
<идентификатор сеанса> 32768 </session-id>
<маркер сеанса> 18wA0TtGmDxPKPQCJywC7fB7EWLCEgz-
ZtjYpAyXx2yJH0H3G3H8t5xpBOx3Ixag </session-token>
<подлинный идентификатор = "успех">
<идентификатор сообщения = "0" param1 = "" param2 = "">
</сообщение>
</аутентификация>

IKEv2-PROTO-3: (6): Построение пакета для шифрования;

ASA создает третий запрос EAP в обмене.
Пакет EAP содержит:

1. **Код: запрос** - Этот код передается средством проверки подлинности узлу.
2. **идентификатор: 3** - идентификатор помогает совпадать с ответами EAP с запросами. Здесь значение равняется 3, который указывает, что это - третий пакет в обмене. Этот пакет имеет 'подлинный

config' тип 'завершенных'; ASA получил ответ, и обмен EAP завершен.

3. **Длина: 4235** - Длина пакета EAP включает код, идентификатор, длину и данные EAP.
4. **Данные EAP**.

Информационное наполнение **ENCR**:
Это информационное наполнение дешифровано, и его содержание проанализировано как дополнительные информационные наполнения.

```
содержание:
 EAP Следующее информационное наполнение: NONE,
зарезервированный: 0x0, длина: 4239
  Код: запрос: идентификатор: 3, длина: 4235
  Введите : Неизвестный - 254
Данные EAP: 4230 байтов

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF
i0:f0] m_id: 0x3
IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r:
FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi:
FC696330E6B94D7F
IKEv2-PROTO-4: Следующее информационное наполнение:
ENCR, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, флаги: ОТВЕТ
MSG РЕСПОНДЕНТА
IKEv2-PROTO-4: Идентификатор сообщения: 0x3, длина: 4300
 ENCR Следующее информационное наполнение: EAP,
зарезервированный: 0x0, длина: 4272
Зашифрованный data&colon; 4268 байтов
IKEv2-PROTO-5: (6): Фрагментируя пакет, MTU Фрагмента:
544, Количество фрагментов: 9, ID Фрагмента: 2
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
```

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000003
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000003 CurState: Событие R_BLD_EAP_REQ:
EV_START_TMR
IKEv2-PROTO-3: (6): Стартовый таймер для ожидания
пользовательского сообщения аутентификации (120 сек.)
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000003 CurState: Событие R_WAIT_EAP_RESP:
EV_NO_EVENT
****

Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnagent

Описание: **Текущий профиль: Anyconnect-ikev2.xml**
Полученные параметры конфигурации сеанса VPN:
Поддержите Установленными: включенный
Параметр прокси: не модифицировать
Прокси-сервер: нет
URL PAC прокси: нет
Исключения для прокси: нет
Блокировка прокси: включенный
Разделение Исключает: предпочтение доступа к локальной сети отключено
Разделение Включает: отключенный
Разделение DNS: отключенный
Подстановочный знак Локальной сети: предпочтение доступа к локальной сети отключено
Правила межсетевого экрана: нет
Адрес клиента: 10.2.2.1
Клиентская маска: 255.0.0.0
Клиентский Адрес IPv6: неизвестный
Клиентская Маска IPv6: неизвестный
MTU: 1406
Поддержка активности IKE: 20 секунд
DPD IKE: 30 секунд
Окончание времени сеанса: 0 секунд
Таймаут разъединения: 1800 секунд
Время простоя: 1800 секунд
Сервер: неизвестный
Хост MUS: неизвестный
Пользовательское сообщение DAP: нет
Карантинное Состояние: отключенный
Всегда На VPN: не отключенный
Продолжительность аренды: 0 секунд

ASA п
парам
настр
конфи
'завер
сообщ
и выд
клиен
VPN.

	Домен по умолчанию: неизвестный Домашняя страница: неизвестный Разъединение Удаления Смарт-карты: включенный Ответ лицензии: неизвестный ********** IKEv2-PLAT-4: **PKT RECV** [IKE_AUTH] [192.168.1.1]:25171-> [10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000004 IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRFi0:f0] m_id: 0x4 IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r: FC696330E6B94D7F] IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0 IKEv2-PROTO-4: **Тип Exchange: IKE_AUTH, флаги: INITIATOR** IKEv2-PROTO-4: Идентификатор сообщения: 0x4, длина: 252 IKEv2-PROTO-5: (6): Запрос имеет mess_id 4; ожидаемый 4 до 4
Клиент передает пакет инициатора с информационным наполнением EAP. Пакет EAP содержит: 1. **Код: ответ** - Этот код передается узлом средству проверки подлинности в ответ на запрос EAP. 2. **идентификатор: 3** - идентификатор помогает совпадать с ответами EAP с запросами. Здесь значение равняется 3, который указывает, что это - ответ на запрос, ранее отправленный ASA (средство проверки подлинности). ASA теперь получает ответный пакет от клиента, который имеет 'подлинный config' тип 'ack'; этот ответ подтверждает EAP 'завершенное' сообщение, передаваемое ранее ASA. 3. **Длина: 173** - Длина пакета EAP включает код, идентификатор, длину и данные EAP. 4. **Данные EAP**.	РЕАЛЬНЫЙ Дешифрованный packet:Data: 177 байтов **EAP** Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 177 **Код: ответ: идентификатор: 3,** длина: 173 Введите : Неизвестный - 254 **Данные EAP**: 168 байтов
ASA обрабатывает этот пакет. Обмен EAP успешен. ASA готовится передавать туннельную группу конфигурация в следующем пакете, который был ранее запрошен клиентом в	Дешифрованные packet:Data:252 байты IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Событие R_WAIT_EAP_RESP: EV_RECV_AUTH IKEv2-PROTO-3: (6): Остановка таймера для ожидания сообщения аутентификации IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)

информационное наполнение IDI. ASA получает ответный пакет от клиента, который имеет 'подлинный config' тип 'ack'. Это ответ подтверждает EAP 'завершите' сообщение, которое передавалось ASA ранее.

Соответствующая конфигурация:

```
tunnel-group ASA-IKEV2
type remote-access
tunnel-group ASA-IKEV2
general-attributes
 address-pool webvpn1
 authorization-server-group
 LOCAL default-group-policy
ASA-IKEV2
tunnel-group ASA-IKEV2
webvpn-attributes
 group-alias ASA-IKEV2
enable
```

Обмен EAP теперь успешен. Пакет EAP содержит:

1. **Код**: **успех** - Этот код передаваемый средством проверки подлинности узел после завершения EAP authentication method. Это указывает, что узел имеет аутентифицируемый успешно на средство проверки подлинности.
2. **идентификатор: 3** - идентификатор помогает совпадать Ответы EAP с запросами. Здесь значение равняется 3, который указывает, что это - ответ на запрос, ранее отправленный

MsgID = 00000004 CurState: Событие R_WAIT_EAP_RESP: EV_RECV_EAP_RESP
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000004 CurState: Событие R_PROC_EAP_RESP: EV_PROC_MSG
IKEv2-PROTO-2: (6): **Обработка ответа EAP**
Полученное сообщение XML ниже от клиента
<? версия xml = "1.0" кодирование = "UTF 8"?>
<подлинный config клиент = "vpn" **вводит = "ack"**>
<device-id> победа </device-id>
<версия, кто = "vpn"> 3.0.1047 </версия>
</config-auth>

IKEv2-PLAT-3: (6) набор aggrAuthHdl к 0x2000
IKEv2-PLAT-3: (6) **набор tg_name к: ASA-IKEV2**
IKEv2-PLAT-3: (6) **tunn набор типа группы к: RA**
IKEv2-PLAT-1: **EAP:Authentication successful**
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000004 CurState: Событие R_PROC_EAP_RESP: EV_RECV_EAP_SUCCESS
IKEv2-PROTO-2: (6): Передача сообщения о статусе EAP
IKEv2-PROTO-3: (6): Построение пакета для шифрования; содержание:
EAP Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 8
Код: успешно: идентификатор: 3, длина: 4

IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRFi0:f0] m_id: 0x4
IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r: FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F
IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, флаги: ОТВЕТ MSG РЕСПОНДЕНТА
IKEv2-PROTO-4: Идентификатор сообщения: 0x4, длина: 76
ENCR Следующее информационное наполнение: EAP, зарезервированный: 0x0, длина: 48
Зашифрованный data: 44 байта

IKEv2-PLAT-4: **ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]**
[10.0.0.1]:4500-> [192.168.1.1]:25171 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000004
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000004 CurState: Событие R_PROC_EAP_RESP: EV_START_TMR
IKEv2-PROTO-3: (6): Стартовый таймер для ожидания

ASA (средство проверки подлинности). Третий набор из пакетов в обмене был успешный, и обмен EAP !--- произведено. 3. **Длина: 4** - длина EAP пакет включает код, идентификатор, длина и данные EAP. 4. **Данные EAP**.	сообщения аутентификации (30 сек.) IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000004 CurState: Событие **R_WAIT_EAP_AUTH_VERIFY**: EV_NO_EVENT
Так как обмен EAP успешен, клиент передает пакет инициатора IKE_AUTH с информационным наполнением AUTH. Информационное наполнение AUTH генерируется от общего секретного ключа.	IKEv2-PLAT-4: PKT RECV [IKE_AUTH] [192.168.1.1]:25171-> [10.0.0.1]:4500 InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f MID=00000005 IKEv2-PROTO-3: Rx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF i0:f0] m_id: 0x5 IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r: FC696330E6B94D7F] IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi: FC696330E6B94D7F IKEv2-PROTO-4: Следующее информационное наполнение: ENCR, версия: 2.0 IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, **флаги: INITIATOR** IKEv2-PROTO-4: Идентификатор сообщения: 0x5, длина: 92 IKEv2-PROTO-5: (6): Запрос имеет mess_id 5; ожидаемый 5 до 5
Когда Аутентификация eap задана или подразумеваемый клиентским профилем и профиль не содержит <IKEIdentity> элемент, клиент передает ID_GROUP вводит информационное наполнение IDI с неподвижная строка * $AnyConnectClient$*. ASA обрабатывает это сообщение. **Соответствующая**	РЕАЛЬНЫЕ Дешифрованные packet:Data:28 байты **AUTH** Следующее информационное наполнение: NONE, зарезервированный: 0x0, длина: 28 **Подлинный PSK метода**, зарезервированный: 0x0, зарезервированный 0x0 **Подлинные данные**: 20 байтов Дешифрованный packet:Data: 92 байта IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие R_WAIT_EAP_AUTH_VERIFY: EV_RECV_AUTH IKEv2-PROTO-3: (6): Остановка таймера для ожидания сообщения аутентификации IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_GET_EAP_KEY IKEv2-PROTO-2: (6): Передайте AUTH, для проверки узла после обмена EAP IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)

конфигурация:

```
crypto dynamic-map dynmap 1000
set ikev2 ipsec-proposal 3des
crypto map crymap 10000
ipsec-isakmp dynamic dynmap
crypto map crymap interface
outside
```

MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_VERIFY_AUTH
IKEv2-PROTO-3: (6): **Проверьте данные проверки подлинности**
IKEv2-PROTO-3: (6): **Используйте общий ключ для идентификатора * $AnyConnectClient$*, ключевой len 20**
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_GET_CONFIG_MODE
IKEv2-PLAT-3: ответ Режима конфигурации помещен в очередь
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-3: PSH: клиентская версия операционной системы client=AnyConnect client-version=3.0.1047 client-os=Windows =
IKEv2-PLAT-3: ответ Режима конфигурации завершен
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_OK_GET_CONFIG
IKEv2-PROTO-3: (6): Имейте данные режима конфигурации для передачи
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_CHK4_IC
IKEv2-PROTO-3: (6): Обработка исходного контакта
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_CHK_REDIRECT
IKEv2-PROTO-5: (6): проверка Перенаправления уже сделана для этого сеанса, пропустив его
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_PROC_SA_TS
IKEv2-PROTO-2: (6): **Обработка сообщения аутентификации**
IKEv2-PLAT-1: **Криптокарта: dynmap seq 1000 Карты. Отрегулированный селектор с помощью назначенного IP - адреса**
IKEv2-PLAT-3: **Криптокарта: соответствие на динамической схеме dynmap seq 1000**
IKEv2-PLAT-3: безопасная пересылка (PFS) отключена для соединения RA
IKEv2-PROTO-3: (6):
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH: EV_NO_EVENT
IKEv2-PLAT-2: Полученный обратный вызов SPI PFKEY для

SPI 0x30B848A4, ошибочной ЛЖИ
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_VERIFY_AUTH:
EV_OK_RECD_IPSEC_RESP
IKEv2-PROTO-2: (6): **Обработка сообщения аутентификации**

ASA создает ответное сообщение IKE_AUTH с SA, TSI и информационными наполнениями TSr.
Пакет респондента IKE_AUTH содержит:

1. **Заголовок ISAKMP** - SPI/версия/флаги.
2. **Информационное наполнение AUTH** - С выбранным методом аутентификации.
3. **CFG** - CFG_REQUEST/CFG_REPLY позволяет оконечной точке IKE запрашивать информацию у своего узла. Если атрибут в информационном наполнении конфигурации CFG_REQUEST не является нулевой длиной, это взято в качестве предложения для того атрибута. Информационное наполнение конфигурации CFG_REPLY может возвратить то значение или новое. Это может также добавить новые атрибуты и не включать некоторые запрошенные. Просители игнорируют возвращенные атрибуты, которые они не распознают. ASA отвечает клиенту с конфигурацией туннеля

IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие **R_BLD_AUTH**:
EV_MY_AUTH_METHOD
IKEv2-PROTO-3: (6): **Получите мой метод аутентификации**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_BLD_AUTH:
EV_GET_PRESHR_KEY
IKEv2-PROTO-3: (6): **Получите общий ключ узла для * $AnyConnectClient$***
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_BLD_AUTH:
EV_GEN_AUTH
IKEv2-PROTO-3: (6): **Генерируйте мои данные проверки подлинности**
IKEv2-PROTO-3: (6): **Используйте общий ключ для идентификатора hostname=ASA-IKEV2, ключевого len 20**
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_BLD_AUTH:
EV_CHK4_SIGN
IKEv2-PROTO-3: (6): Получите мой метод аутентификации
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие R_BLD_AUTH:
EV_OK_AUTH_GEN
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие
R_BLD_EAP_AUTH_VERIFY: EV_GEN_AUTH
IKEv2-PROTO-3: (6): Генерируйте мои данные проверки подлинности
IKEv2-PROTO-3: (6): Используйте общий ключ для идентификатора hostname=ASA-IKEV2, ключевого len 20
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие
R_BLD_EAP_AUTH_VERIFY: EV_SEND_AUTH
IKEv2-PROTO-2: (6): **Передайте AUTH, для проверки узла после обмена EAP**
IKEv2-PROTO-3: ESP Предложение: 1, размер SPI: 4 (Согласование IPsec),
Цифра. преобразовывает: 3
  CBC AES SHA96
IKEv2-PROTO-5: Конструкция Уведомляет Информационное

atrributes в пакете CFG_REPLY.

4. **SAr2** - SAr2 инициирует SA, который подобен обмену набора преобразований фазы 2 в IKEv1.
5. **TSI** и **TSr** - селекторы трафика инициатора и респондента содержат, соответственно, адрес источника и назначения инициатора и респондента, чтобы передать и получить зашифрованный поток данных. Диапазон адресов указывает, что туннелирован весь трафик к и из того диапазона. Если предложение приемлемо для респондента, оно передает идентичные информационные наполнения TS обратно.

Информационное наполнение **ENCR**:
Это информационное наполнение дешифровано, и его содержание проанализировано как дополнительные информационные наполнения.

наполнение: ESP_TFC_NO_SUPPORTIKEv2-PROTO-5:
Конструкция Уведомляет Информационное наполнение:
NON_FIRST_FRAGSIKEv2-PROTO-3: (6): Построение пакета для шифрования; содержание:
AUTH Следующее информационное наполнение: CFG, зарезервированный: 0x0, длина: 28
Подлинный PSK метода, зарезервированный: 0x0, зарезервированный 0x0
Аутентификация data: 20 байтов
CFG Следующее информационное наполнение: SA, зарезервированный: 0x0, длина: 4196
тип cfg: **CFG_REPLY,** зарезервированный: 0x0, зарезервированный: 0x0

тип attrib: внутренний адрес IP4, длина: 4

01 01 01 01
тип attrib: внутренняя маска подсети IP4, длина: 4

00 00 00 00
тип attrib: истечение внутреннего адреса, длина: 4

00 00 00 00
тип attrib: версия приложения, длина: 16

41 53 41 20 31 30 30 2e 37 28 36 29 31 31 36 00
тип attrib: Неизвестный - 28704, длина: 4

00 00 00 00
тип attrib: Неизвестный - 28705, длина: 4

00 00 07 08
тип attrib: Неизвестный - 28706, длина: 4

00 00 07 08
тип attrib: Неизвестный - 28707, длина: 1

01
тип attrib: Неизвестный - 28709, длина: 4

00 00 00 1e
тип attrib: Неизвестный - 28710, длина: 4

00 00 00 14
тип attrib: Неизвестный - 28684, длина: 1

01
тип attrib: Неизвестный - 28711, длина: 2

05 7e
тип attrib: Неизвестный - 28679, длина: 1

00

тип attrib: Неизвестный - 28683, длина: 4

80 0b 00 01
тип attrib: Неизвестный - 28725, длина: 1

00
тип attrib: Неизвестный - 28726, длина: 1

00
тип attrib: Неизвестный - 28727, длина: 4056

3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3-й 22 31
2e 30 22 20 65 6e 63 6f 64 69 6e 67 3-х 22 55 54
46 2-х 38 22 3f 3e 3c 63 6f 6e 66 69 67 2-х 61 75
74 68 20 63 6c 69 65 6e 74 3-х 22 76 70 6e 22 20
74 79 70 65 3-х 22 63 6f 6d 70 6c 65 74 65 22 3e
3c 76 65 72 73 69 6f 6e 20 77 68 6f 3-й 22 73 67
22 3e 31 30 30 2e 37 28 36 29 31 31 36 3c 2f 76
65 72 73 69 6f 6e 3e 3c 73 65 73 73 69 6f 6e 2-й
69 64 3e 38 31 39 32 3c 2f 73 65 73 73 69 6f 6e
<надрез>
72 6f 66 69 6c 65 2-х 6d 61 6e 69 66 65 73 74 3e
3c 2f 63 6f 6e 66 69 67 3e 3c 2f 63 6f 6e 66 69
67 2-х 61 75 74 68 3e 00
тип attrib: Неизвестный - 28729, длина: 1

00
SA Следующее информационное наполнение: TSI, зарезервированный: 0x0, длина: 44
IKEv2-PROTO-4: последнее предложение: 0x0, зарезервированный: 0x0, длина: 40
Предложение: 1, Идентификатор протокола: ESP, размер SPI: 4, #trans: 3
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 12
введите : 1, зарезервированный: 0x0, идентификатор: CBC AES
IKEv2-PROTO-4 : последнее преобразование: 0x3, зарезервированный: 0x0: длина: 8
введите : 3, зарезервированный: 0x0, идентификатор: SHA96
IKEv2-PROTO-4 : последнее преобразование: 0x0, зарезервированный: 0x0: длина: 8
введите : 5, зарезервированный: 0x0, идентификатор:

TSI Следующее информационное наполнение: TSr, зарезервированный: 0x0, длина: 24
Цифра TSs: 1, зарезервированный 0x0, зарезервированный 0x0
Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор: 0, длина: 16
начальный порт: 0, оконечный порт: 65535
запустите адрес: 10.2.2.1, конечный адрес: 10.2.2.1
TSr Следующее информационное наполнение: NOTIFY,

```
зарезервированный: 0x0, длина: 24
  Цифра TSs: 1, зарезервированный 0x0, зарезервированный
0x0
  Тип TS: TS_IPV4_ADDR_RANGE, первичный идентификатор:
0, длина: 16
  начальный порт: 0, оконечный порт: 65535
  запустите адрес: 0.0.0.0, конечный адрес: 255.255.255.255
IKEv2-PROTO-3: Tx [L 10.0.0.1:4500/R 192.168.1.1:25171/VRF
i0:f0] m_id: 0x5
IKEv2-PROTO-3: HDR [i:58AFF71141BA436B - r:
FC696330E6B94D7F]
IKEv2-PROTO-4: IKEV2 HDR ispi: 58AFF71141BA436B - rspi:
FC696330E6B94D7F
IKEv2-PROTO-4: Следующее информационное наполнение:
ENCR, версия: 2.0
IKEv2-PROTO-4: Тип Exchange: IKE_AUTH, флаги: ОТВЕТ
MSG РЕСПОНДЕНТА
IKEv2-PROTO-4: Идентификатор сообщения: 0x5, длина: 4396
 ENCR Следующее информационное наполнение: AUTH,
зарезервированный: 0x0, длина: 4368
Зашифрованный data&colon; 4364 байта
```

ASA отсылает это ответное сообщение IKE_AUTH, которое фрагментировано в девять пакетов. Обмен IKE_AUTH завершен.

```
IKEv2-PROTO-5: (6): Фрагментируя пакет, MTU Фрагмента:
544, Количество фрагментов: 9, ID Фрагмента: 3
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
```

InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PLAT-4: ПЕРЕДАВАЕМЫЙ PKT [IKE_AUTH]
[10.0.0.1]:4500-> [192.168.1.1]:25171
InitSPI=0x58aff71141ba436b RespSPI=0xfc696330e6b94d7f
MID=00000005
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие AUTH_DONE: EV_OK
IKEv2-PROTO-5: (6): Действие: Action_Null
IKEv2-PROTO-5: (6): Трассировка SM-> SA:
I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R)
MsgID = 00000005 CurState: Событие **AUTH_DONE**:
EV_PKI_SESH_CLOSE
****

Клиен
IP - бе
соеди
устан
также
профи
польз
ASA.

Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnagent

Описание: Функция: ikev2_log
Файл:.\ikev2_anyconnect_osal.cpp
Линия: 2730
IP - безопасное соединение было установлено.
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnagent

Описание: Регистрация сеанса IPSec:
Шифрование: CBC AES
PRF: SHA1
HMAC: SHA96
Локальный подлинный метод: PSK
Удаленный подлинный метод: PSK
Идентификатор последовательности: 0
Размер ключа: 192
Группа DH: 1
Повторно введите время: 4294967 секунд
Local Address: 192.168.1.1
Удаленный адрес: 10.0.0.1
Локальный порт: 4500
Удаленный порт: 4500
Идентификатор сеанса: 1
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnui

Описание: **Профиль, настроенный на защищенном шлюзе:
Anyconnect-ikev2.xml**

****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnui

Описание: Информация о типе сообщения, передаваемая пользователю:
Установление сеанса VPN...
****
----------Обмен IKE_AUTH заканчивает----------
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpndownloader

Описание: Функция: ProfileMgr:: loadProfiles
Файл:..\Api\ProfileMgr.cpp
Линия: 148
Загруженные профили:
C : \Documents и AnyConnect Settings\All Users\Application Data\Cisco\Cisco безопасная мобильность Client\Profile\anyconnect-ikev2.xml
****
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpndownloader

Описание: Текущие настройки:
ServiceDisable: fALSE
CertificateStoreOverride: fALSE
CertificateStore: все
ShowPreConnectMessage: fALSE
AutoConnectOnStart: fALSE
MinimizeOnConnect: tRUE
LocalLanAccess: fALSE
AutoReconnect: tRUE
AutoReconnectBehavior: DisconnectOnSuspend
UseStartBeforeLogon: fALSE
AutoUpdate: tRUE
RSASecurIDIntegration: автоматический
WindowsLogonEnforcement: SingleLocalLogon
WindowsVPNEstablishment: LocalUsersOnly
ProxySettings: собственный компонент
AllowLocalProxyConnections: tRUE
PPPExclusion: отключить
PPPExclusionServerIP:
AutomaticVPNPolicy: fALSE
TrustedNetworkPolicy: разъединение

Проф
загруж
клиен
клиен
IP-адр
клиен
активн
адапт

UntrustedNetworkPolicy: подключение
TrustedDNSDomains:
TrustedDNSServers:
Алвейсон: fALSE
ConnectFailurePolicy: закрытый
AllowCaptivePortalRemediation: fALSE
CaptivePortalRemediationTimeout: 5
ApplyLastVPNLocalResourceRules: fALSE
AllowVPNDisconnect: tRUE
EnableScripting: fALSE
TerminateScriptOnNextEvent: fALSE
EnablePostSBLOnConnectScript: tRUE
AutomaticCertSelection: tRUE
Ретэйнвпнонлогофф: fALSE
UserEnforcement: SameUserOnly
EnableAutomaticServerSelection: fALSE
AutoServerSelectionImprovement: 20
AutoServerSelectionSuspendTime: 4
Время ожидания при аутентификации: 12
SafeWordSofTokenIntegration: fALSE
AllowIPsecOverSSL: fALSE
ClearSmartcardPin: tRUE
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnui

Описание: Информация о типе сообщения, передаваемая пользователю:
Установление VPN - Исследование системы...
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnui

Описание: Информация о типе сообщения, передаваемая пользователю:
Установление VPN - Активация адаптера VPN...
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnagent

Описание: Функция: CVirtualAdapter:: DoRegistryRepair
Файл:.\WindowsVirtualAdapter.cpp
Линия: 1869
Найденная Клавиша CTRL ВА:
SYSTEM\CurrentControlSet\ENUM\ROOT\NET\0000\Control
****
Дата : 23.04.2013

Время : 16:25:07
Введите : Информация
Источник: acvpnagent

Описание: **Был обнаружен новый сетевой интерфейс.**
****
Дата : 23.04.2013
Время : 16:25:07
Введите : Информация
Источник: acvpnagent

Описание: Функция: CRouteMgr:: logInterfaces
Файл:.\RouteMgr.cpp
Линия: 2076
Вызванная Функция: logInterfaces
Код возврата: 0 (0x00000000)
Описание: Список интерфейсов IP-адреса:
10.2.2.1
192.168.1.1
****
Дата : 23.04.2013
Время : 16:25:08
Введите : Информация
Источник: acvpnagent

Описание: Конфигурация хоста:
Общий адрес: 192.168.1.1
Общая маска: 255.255.255.0
Частный адрес: 10.2.2.1
Частная маска: 255.0.0.0
Частный адрес IPv6: Н/Д
Частная маска IPv6: Н/Д
Удаленные узлы: 10.0.0.1 (порт TCP 443, порт 500 UDP), 10.0.0.1 (порт 4500 UDP)
Частные сети: нет
Открытые сети: нет
Tunnel mode: да
****

Соединение введено в базу данных Сопоставления безопасности (SA), и статус ЗАРЕГИСТРИРОВАН. ASA также выполняет некоторые проверки как stats карты общего доступа (CAC), присутствие двойных SA, и устанавливает значения как Dead Peer Detection (DPD) и т.д.

IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие AUTH_DONE: **EV_INSERT_IKE**
IKEv2-PROTO-2: (6): **SA создан; вставка SA в базу данных**
IKEv2-PLAT-3:
СТАТУС СОЕДИНЕНИЯ: _____ включен... одноранговый узел: 192.168.1.1:25171, phase1_id: * $AnyConnectClient$*
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие AUTH_DONE: **EV_REGISTER_SESSION**
IKEv2-PLAT-3: (6) **набор имени пользователя к: Anu**
IKEv2-PLAT-3:
СТАТУС СОЕДИНЕНИЯ: ЗАРЕГИСТРИРОВАННЫЙ...

одноранговый узел: 192.168.1.1:25171, **phase1_id: * $AnyConnectClient$***
IKEv2-PROTO-3: (6): Инициализация DPD, настроенного в течение 10 секунд
IKEv2-PLAT-3: (6) набор mib_index к: 4501
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие AUTH_DONE: EV_GEN_LOAD_IPSEC
IKEv2-PROTO-3: (6): материал КЛЮЧА IPSEC Загрузки
IKEv2-PLAT-3: Криптокарта: соответствие на динамической схеме dynmap seq 1000
IKEv2-PLAT-3: (6) **DPD Время Max будет: 30**
IKEv2-PLAT-3: (6) **DPD Время Max будет: 30**
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие AUTH_DONE: EV_START_ACCT
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие AUTH_DONE: EV_CHECK_DUPE
IKEv2-PROTO-3: (6): **Проверка двойной SA**
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: Событие AUTH_DONE: EV_CHK4_ROLE
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: ГОТОВОЕ Событие: EV_R_UPDATE_CAC_STATS
IKEv2-PLAT-5: Новый запрос ikev2 sa активирован
IKEv2-PLAT-5: Декрементный счет для входящего согласования
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: ГОТОВОЕ Событие: EV_R_OK
IKEv2-PROTO-3: (6): Стартовый таймер для удаления контекста согласования
IKEv2-PROTO-5: (6): Трассировка SM-> SA: I_SPI=58AFF71141BA436B R_SPI=FC696330E6B94D7F (R) MsgID = 00000005 CurState: ГОТОВОЕ Событие: EV_NO_EVENT
IKEv2-PLAT-2: Полученные PFKEY добавляют SA для SPI 0x77EE5348, ошибочной ЛЖИ
IKEv2-PLAT-2: Полученные PFKEY обновляют SA для SPI 0x30B848A4, ошибочной ЛЖИ
****
Дата : 23.04.2013
Время : 16:25:08
Введите : Информация
Источник: acvpnagent

Клиен
тунне
готов
трафи

Описание: **VPN-подключение было установлено и может теперь передать данные.**
****
Дата : 23.04.2013
Время : 16:25:08
Введите : Информация
Источник: acvpnui

Описание: Информация о типе сообщения, передаваемая пользователю:
Установление VPN - система Настройки...
****
Дата : 23.04.2013
Время : 16:25:08
Введите : Информация
Источник: acvpnui

Описание: Информация о типе сообщения, передаваемая пользователю:
Установление VPN...
****
Дата : 23.04.2013
Время : 16:25:37
Введите : Информация
Источник: acvpnagent

Файл:.\IPsecProtocol.cpp
Линия: 945
Туннель IPSec установлен
****

Туннельная проверка

AnyConnect

Пример выходных данных от **anyconnect** команды **подробности покажите vpn-sessiondb**:

```
Session Type: AnyConnect Detailed

Username    : Anu                   Index       : 2
Assigned IP : 10.2.2.1               Public IP   : 192.168.1.1
Protocol    : IKEv2 IPsecOverNatT AnyConnect-Parent
License     : AnyConnect Premium
Encryption  : AES192 AES256         Hashing     : none SHA1 SHA1
Bytes Tx    : 0                     Bytes Rx    : 11192
Pkts Tx     : 0                     Pkts Rx     : 171
Pkts Tx Drop : 0                     Pkts Rx Drop : 0
Group Policy : ASA-IKEV2             Tunnel Group : ASA-IKEV2
Login Time  : 22:06:24 UTC Mon Apr 22 2013
Duration    : 0h:02m:26s
Inactivity  : 0h:00m:00s
```

```
NAC Result  : Unknown
VLAN Mapping : N/A                    VLAN        : none

IKEv2 Tunnels: 1
IPsecOverNatT Tunnels: 1
AnyConnect-Parent Tunnels: 1

AnyConnect-Parent:
 Tunnel ID   : 2.1
 Public IP   : 192.168.1.1
 Encryption  : none                   Auth Mode   : userPassword
 Idle Time Out: 30 Minutes             Idle TO Left : 27 Minutes
 Client Type : AnyConnect
Client Ver  : 3.0.1047
IKEv2:
 Tunnel ID   : 2.2
 UDP Src Port : 25171                  UDP Dst Port : 4500
 Rem Auth Mode: userPassword
 Loc Auth Mode: rsaCertificate
 Encryption  : AES192                 Hashing     : SHA1
 Rekey Int (T): 86400 Seconds          Rekey Left(T): 86254 Seconds
 PRF         : SHA1                   D/H Group   : 1
 Filter Name :
 Client OS   : Windows
IPsecOverNatT:
 Tunnel ID   : 2.3
 Local Addr  : 0.0.0.0/0.0.0.0/0/0
 Remote Addr : 10.2.2.1/255.255.255.255/0/0
 Encryption  : AES256                 Hashing     : SHA1
  Encapsulation: Tunnel
 Rekey Int (T): 28800 Seconds          Rekey Left(T): 28654 Seconds
  Rekey Int (D): 4608000 K-Bytes       Rekey Left(D): 4607990 K-Bytes
  Idle Time Out: 30 Minutes            Idle TO Left : 29 Minutes
 Bytes Tx    : 0                      Bytes Rx    : 11192
  Pkts Tx     : 0                      Pkts Rx     : 171
 NAC:
 Reval Int (T): 0 Seconds              Reval Left(T): 0 Seconds
 SQ Int (T)  : 0 Seconds              EoU Age(T)  : 146 Seconds
 Hold Left (T): 0 Seconds              Posture Token:
Redirect URL :
```

ISAKMP

Пример выходных данных от **команды show crypto ikev2 sa**:

```
ASA-IKEV2# show crypto ikev2 sa

IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote    Status        Role
 55182129   10.0.0.1/4500        192.168.1.1/25171     READY   RESPONDER
    Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
  Life/Active Time: 86400/112 sec
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
         remote selector 10.2.2.1/0 - 10.2.2.1/65535
         ESP spi in/out: 0x30b848a4/0x77ee5348
```

Пример выходных данных от **подробной** команды **покажите крипто-ikev2 sa**:

```
ASA-IKEV2# show crypto ikev2 sa detail
```

```
IKEv2 SAs:

Session-id:2, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id                Local                Remote    Status        Role
 55182129   10.0.0.1/4500        192.168.1.1/25171     READY   RESPONDER
     Encr: AES-CBC, keysize: 192, Hash: SHA96, DH Grp:1, Auth sign: RSA, Auth verify: EAP
     Life/Active Time: 86400/98 sec
     Session-id: 2
     Status Description: Negotiation done
     Local spi: FC696330E6B94D7F      Remote spi: 58AFF71141BA436B
     Local id: hostname=ASA-IKEV2
     Remote id: *$AnyConnectClient$*
     Local req mess id: 0             Remote req mess id: 9
     Local next mess id: 0            Remote next mess id: 9
     Local req queued: 0              Remote req queued: 9      Local window:
1                 Remote window: 1
     DPD configured for 10 seconds, retry 2
     NAT-T is detected outside
     Assigned host addr: 10.2.2.1
Child sa: local selector 0.0.0.0/0 - 255.255.255.255/65535
          remote selector 10.2.2.1/0 - 10.2.2.1/65535
          ESP spi in/out: 0x30b848a4/0x77ee5348
         AH spi in/out: 0x0/0x0
         CPI in/out: 0x0/0x0
           Encr: AES-CBC, keysize: 256, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

IPSec

Пример выходных данных от **команды show crypto ipsec sa**:

```
ASA-IKEV2# show crypto ipsec sa
interface: outside
   Crypto map tag: dynmap, seq num: 1000, local addr: 10.0.0.1

  local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
     remote ident (addr/mask/prot/port): (10.2.2.1/255.255.255.255/0/0)
     current_peer: 192.168.1.1, username: Anu
     dynamic allocated peer ip: 10.2.2.1

     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
   #pkts decaps: 163, #pkts decrypt: 108, #pkts verify: 108
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
     #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
     #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
     #send errors: 0, #recv errors: 55

    local crypto endpt.: 10.0.0.1/4500, remote crypto endpt.: 192.168.1.1/25171
     path mtu 1488, ipsec overhead 82, media mtu 1500
     current outbound spi: 77EE5348
     current inbound spi : 30B848A4

 inbound esp sas:
    spi: 0x30B848A4 (817383588)
       transform: esp-aes-256 esp-sha-hmac no compression
       in use settings ={RA, Tunnel, NAT-T-Encaps, }
       slot: 0, conn_id: 8192, crypto-map: dynmap
       sa timing: remaining key lifetime (sec): 28685
       IV size: 16 bytes
       replay detection support: Y
```

```
    Anti replay bitmap:
    0xFFAD6BED 0x7ABFD5BF
outbound esp sas:
  spi: 0x77EE5348 (2012107592)
     transform: esp-aes-256 esp-sha-hmac no compression
    in use settings ={RA, Tunnel, NAT-T-Encaps, }
     slot: 0, conn_id: 8192, crypto-map: dynmap
     sa timing: remaining key lifetime (sec): 28685
     IV size: 16 bytes
     replay detection support: Y
     Anti replay bitmap:
     0x00000000 0x00000001
```

Дополнительные сведения

- RFC 4306, обмен ключами между сетями (IKEv2) протокол
- RFC 3748, протокол EAP
- RFC 5996, версия протокола 2 (IKEv2) обмена ключами между сетями
- Cisco Systems – техническая поддержка и документация