AnyConnect к головному узлу IOS по IPsec с IKEv2 и примером конфигурации сертификатов

Содержание

Введение

Этот документ предоставляет сведения о том, как достигнуть резервируемого соединения Ipsec от устройства, которое выполняет клиента AnyConnect к маршрутизатору Cisco IOS® с только проверкой подлинности сертификата путем использования платформы FlexVPN.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- FlexVPN
- AnyConnect

Используемые компоненты

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

Головной узел

Маршрутизатор Cisco IOS может быть любым маршрутизатором, способным к выполнению IKEv2, выполнив по крайней мере 15.2 выпусков M&T. Однако необходимо использовать более новый выпуск (см. раздел известных предупреждений), при наличии.

Клиент

AnyConnect 3. выпуск X

Центр сертификации

В данном примере центр сертификации (CA) будет работать 15.2 (3) выпуск T.

Крайне важно, чтобы одни из более новых версий использовались из-за потребности поддержать расширенное использование ключа (EKU).

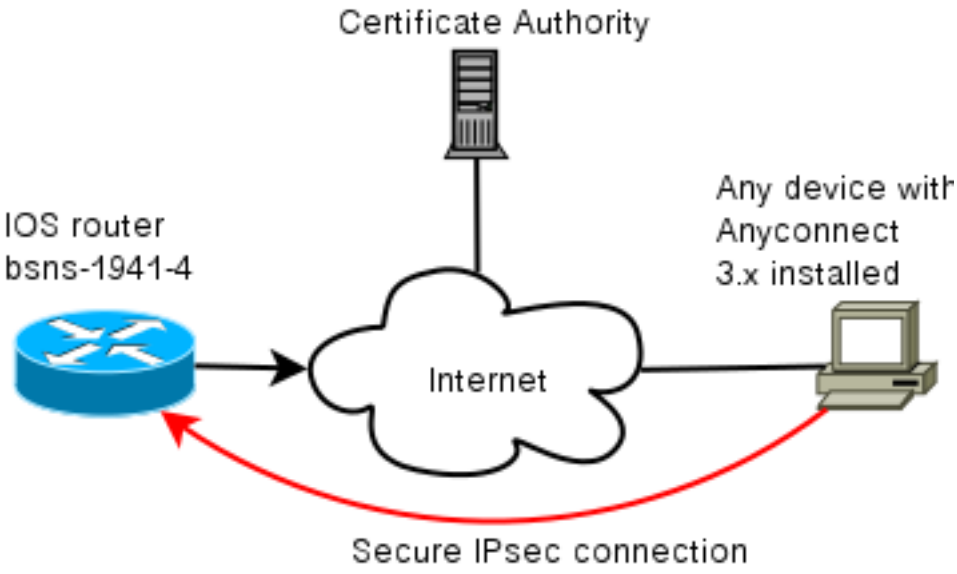
В этих развертываниях маршрутизатор IOS используется в качестве CA. Однако любой на основе стандартов CA, что приложение, способное к использованию EKU, должно быть прекрасным.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.

!--- конфигурацию

Топология сети



(Дополнительный) центр сертификации

Если вы принимаете решение использовать его, ваш маршрутизатор IOS может действовать как CA.

IOS CA конфигурация

Необходимо помнить, что сервер CA должен поместить корректный EKU на сертификаты клиента и сервера. В этой аутентификации сервера случая и клиентско-подлинном EKU были установлены для всех сертификатов.

```
bsns-1941-3#show run | s crypto pki
crypto pki server CISCO
database level complete
database archive pem password 7 00071A1507545A545C
issuer-name cn=bsns-1941-3.cisco.com,ou=TAC,o=cisco
grant auto rollover ca-cert
grant auto
auto-rollover
eku server-auth client-auth
```

Как проверить, был ли корректный EKU установлен на сертификате

В то время как bsns-1941-4 является головным узлом Ipsec, Обратите внимание на то, что bsns-1941-3 является сервером CA. Части выходных данных опущены для краткости.

```
BSNS-1941-4#show crypto pki certificate verbose
Certificate
(...omitted...)

Public Key Algorithm: rsaEncryption
RSA Public Key: (1024 bit)
Signature Algorithm: SHA1 with RSA Encryption
Fingerprint MD5: C3D52BE9 1EE97559 C7323995 3C51DC53
Fingerprint SHA1: 76BC7CD4 F298F8D9 A95338DC E5AF7602 9B57BE31
X509v3 extensions:
X509v3 Key Usage: A0000000
Digital Signature
```

```
Key Encipherment
X509v3 Subject Key ID: 83647B09 D3300A97 577C3E2C AAE7F47C F2D88ADF
X509v3 Authority Key ID: B3CC331D 7159C3CD 27487322 88AC02ED FAF2AE2E
Authority Info Access:
Extended Key Usage:
Client Auth
Server Auth
Associated Trustpoints: CISCO2
Storage: nvram:bsns-1941-3c#5.cer
Key Label: BSNS-1941-4.cisco.com
Key storage device: private config

CA Certificate
(...omitted...)
```

Конфигурация головного узла

Конфигурация головного узла состоит из двух частей: часть PKI и фактический flex/IKEv2.

Конфигурация PKI

Вы заметите тот CN bsns-1941-4. cisco . com используется. Это должно совпасть с надлежащей Записью DNS и должно быть включено в профиль AnyConnect под <hostname>.

```
crypto pki trustpoint CISCO2
enrollment url http://10.48.66.14:80
serial-number
ip-address 10.48.66.15
subject-name cn=bsns-1941-4.cisco.com,ou=TAC,o=cisco
revocation-check none

crypto pki certificate map CMAP 10
subject-name co cisco
```

КРИПТО-/Конфигурация IPSec

Обратите внимание на то, что ваше значение PRF/ЦЕЛОСТНОСТИ в предложении NEEDS для соответствия, что поддержки сертификата. Это, как правило, - SHA-1.

```
crypto ikev2 authorization policy AC
pool AC

crypto ikev2 proposal PRO
encryption 3des aes-cbc-128
integrity sha1
group 5 2

crypto ikev2 policy POL
match fvrf any
proposal PRO

crypto ikev2 profile PRO
match certificate CMAP
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
```

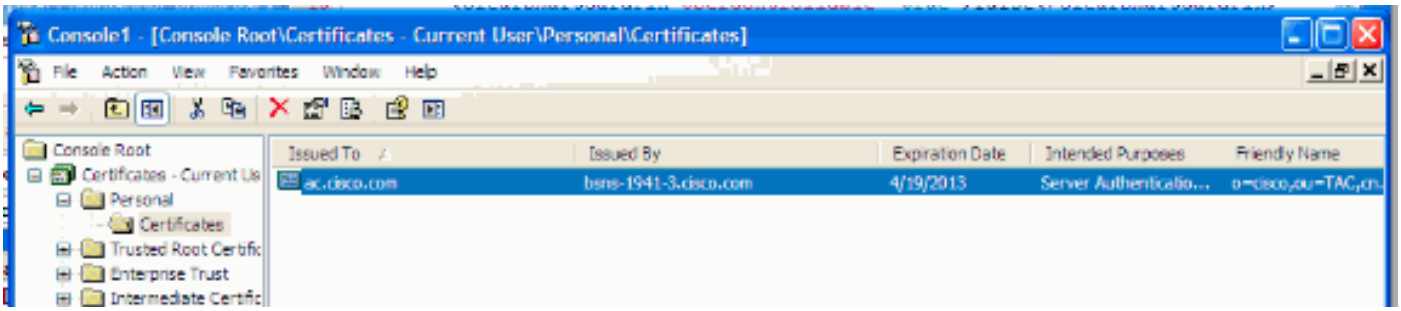
```
virtual-template 1

no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

crypto ipsec profile PRO
set transform-set TRA
set ikev2-profile PRO

interface Virtual-Template1 type tunnel
ip unnumbered GigabitEthernet0/0
tunnel mode ipsec ipv4 tunnel protection ipsec profile PRO
```

Клиент

Конфигурация клиента для успешного Соединения AnyConnect с IKEv2 и сертификатами состоит из двух частей.

Хранилище сертификатов

Когда сертификат должным образом зарегистрирован, можно проверить, что он присутствует или в машине или в персональном хранилище. Помните, что сертификаты клиента также должны иметь EKU.



Профиль AnyConnect

Профиль AnyConnect является длинным и очень простым.

Соответствующая часть должна определить:

1. Хост вы соединяетесь с
2. Тип протокола
3. Аутентификация, которая будет использоваться, когда связано с тем хостом

Что используется:

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
IKE-RSA
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
```

```
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

В поле соединения AnyConnect необходимо предоставить полный FQDN, который является значением, замеченным в `<HostName>`.

Проверка соединения

Некоторая информация опущена для краткости.

```
BSNS-1941-4#show crypto ikev2 sa
IPv4 Crypto IKEv2 SA
Tunnel-id Local Remote fvrf/ivrf Status
2 10.48.66.15/4500 10.55.193.212/65311 none/none READY
Encr: AES-CBC, keysize: 128, Hash: SHA96, DH Grp:5,
Auth sign: RSA, Auth verify: RSA
Life/Active Time: 86400/180 sec


IPv6 Crypto IKEv2 SA

BSNS-1941-4#show crypto ipsec sa

interface: Virtual-Access1
Crypto map tag: Virtual-Access1-head-0, local addr 10.48.66.15

protected vrf: (none)
local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
remote ident (addr/mask/prot/port): (172.16.1.2/255.255.255.255/0/0)
current_peer 10.55.193.212 port 65311
PERMIT, flags={origin_is_acl,}
#pkts encaps: 2, #pkts encrypt: 2, #pkts digest: 2
#pkts decaps: 26, #pkts decrypt: 26, #pkts verify: 26

local crypto endpt.: 10.48.66.15, remote crypto endpt.: 10.55.193.212
path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet0/0
current outbound spi: 0x5C171095(1545015445)
PFS (Y/N): N, DH group: none

inbound esp sas:
spi: 0x8283D0F0(2189676784)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2003, flow_id: Onboard VPN:3, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215478/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)

outbound esp sas:
spi: 0x5C171095(1545015445)
transform: esp-3des esp-sha-hmac ,
in use settings ={Tunnel UDP-Encaps, }
conn id: 2004, flow_id: Onboard VPN:4, sibling_flags 80000040,
crypto map: Virtual-Access1-head-0
sa timing: remaining key lifetime (k/sec): (4215482/3412)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE(ACTIVE)
```

Криптография следующего поколения

Вышеупомянутая конфигурация предоставлена для ссылки для показа минимальной действующей конфигурации. Cisco рекомендует использовать криптографию следующего поколения (NGC), если это возможно.

Текущие рекомендации для миграции могут быть найдены здесь: http://www. cisco . com/web/about/security/intelligence/nextgen_crypto.html

При выборе конфигурации NGC удостоверьтесь что и клиентское программное обеспечение и аппаратная поддержка головного узла это. Поколение 2 ISR и ASR 1000 маршрутизаторов рекомендуются как головные узлы из-за их аппаратной поддержки для NGC.

На стороне AnyConnect, с версии AnyConnect 3.1, поддерживается Комплект NSA B комплект алгоритма.

Известные предупреждения и проблемы

- Не забудьте настраивать эту линию на вашем головном узле IOS: **никакое крипто-ikev2 свидетельство http url**. Ошибка, произведенная IOS и AnyConnect, когда это не настроено, является довольно вводящей в заблуждение.
- Раннее программное обеспечение IOS 15.2M&T с сеансом IKEv2 не могло бы предстать перед аутентификацией RSA-СИГНАЛА. Это может быть отнесено к идентификатору ошибки Cisco CSCtx31294 (только зарегистрированные клиенты). Удостоверьтесь, что выполнили последнее 15.2M или 15.2T программное обеспечение.
- В определенных сценариях IOS не мог бы быть в состоянии выбрать корректную точку доверия для аутентификации. Cisco знает о проблеме, и это исправлено с 15.2 (3) T1 и 15.2 (4) версии M1.
- Если AnyConnect сообщает о сообщении, подобном этому:
```
The client certificate's
cryptographic service provider(CSP)
does not support the sha512 algorithm
```

Затем необходимо удостовериться, что значение ЦЕЛОСТНОСТИ/PRF в предложениях IKEv2 совпадает с тем, что могут обработать сертификаты. В примере конфигурации выше, используется SHA-1.

Дополнительные сведения

- Cisco Systems – техническая поддержка и документация