AnyConnect to IOS Headend Over IPsec mit IKEv2 und Konfigurationsbeispiel für Zertifikate

Inhalt

Einführung

Dieses Dokument enthält Informationen zum Herstellen einer IPsec-geschützten Verbindung von einem Gerät, auf dem der AnyConnect-Client mit einem Cisco IOS®-Router ausgeführt wird, mit ausschließlicher Zertifikatsauthentifizierung unter Verwendung des FlexVPN-Frameworks.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- FlexVPN
- AnyConnect

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

Headend

Der Cisco IOS-Router kann ein beliebiger Router sein, der IKEv2 mit einer M&T-Version von mindestens 15,2 ausführen kann. Sie sollten jedoch eine neuere Version verwenden (siehe Abschnitt mit bekannten Vorbehalten), falls verfügbar.

Client

AnyConnect 3.x-Version

Zertifizierungsstelle

In diesem Beispiel wird die Zertifizierungsstelle (Certificate Authority, CA) die Version 15.2(3)T ausführen.

Es ist wichtig, dass eine der neueren Versionen verwendet wird, da Extended Key Usage (EKU) unterstützt werden muss.

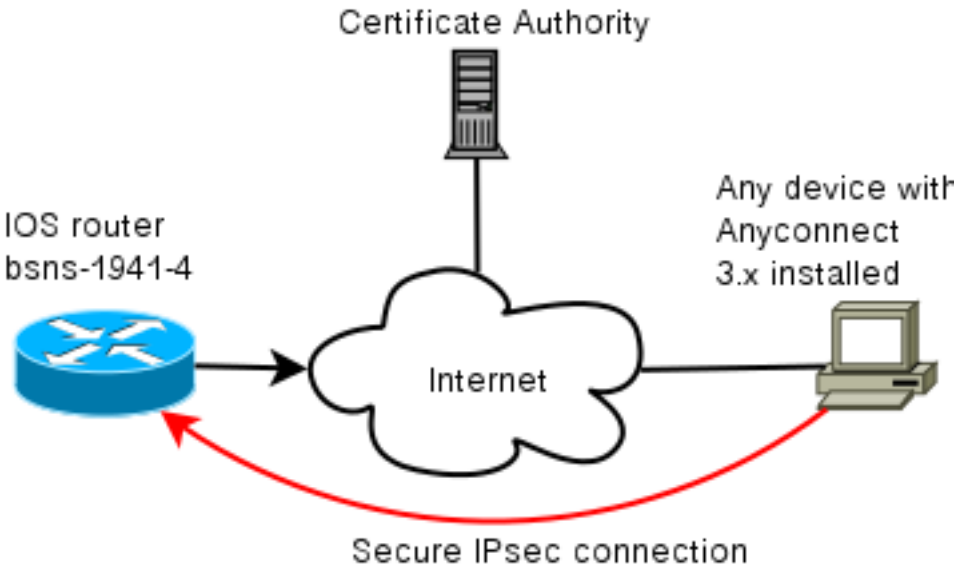
In dieser Bereitstellung wird der IOS-Router als CA verwendet. Allerdings sollte jede standardbasierte CA-Anwendung, die EKU verwenden kann, in Ordnung sein.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration

Netzwerktopologie



Zertifizierungsstelle (optional)

Wenn Sie es verwenden, kann Ihr IOS-Router als CA agieren.

IOS-CA-Konfiguration

Sie müssen sich daran erinnern, dass der CA-Server das korrekte EKU auf die Client- und Server-Zertifikate legen muss. In diesem Fall wurden Server-Auth und Client-Auth EKU für alle Zertifikate festgelegt.

```
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
```

Überprüfung, ob das Zertifikat die korrekte EKU enthält

Beachten Sie, dass bsns-1941-3 der CA-Server ist, während bsns-1941-4 das IPsec-Headend ist. Teile der Ausgabe wurden aus Gründen der Kürze weggelassen.

```
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...)
```

Headend-Konfiguration

Die Headend-Konfiguration besteht aus zwei Teilen: PKI-Teil und tatsächlicher Flex/IKEv2.

PKI-Konfiguration

Sie werden feststellen, dass die CN von bsns-1941-4.cisco.com verwendet wird. Dies muss mit einem geeigneten DNS-Eintrag übereinstimmen und muss unter <Hostname> im AnyConnect-Profil enthalten sein.

```
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
```

Konfiguration von Krypto/IPsec

Beachten Sie, dass Ihre PRF-/Integritätseinstellung im Angebot **NÖTIG** ist, damit sie mit der Unterstützung Ihres Zertifikats übereinstimmt. Dies ist in der Regel 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
```

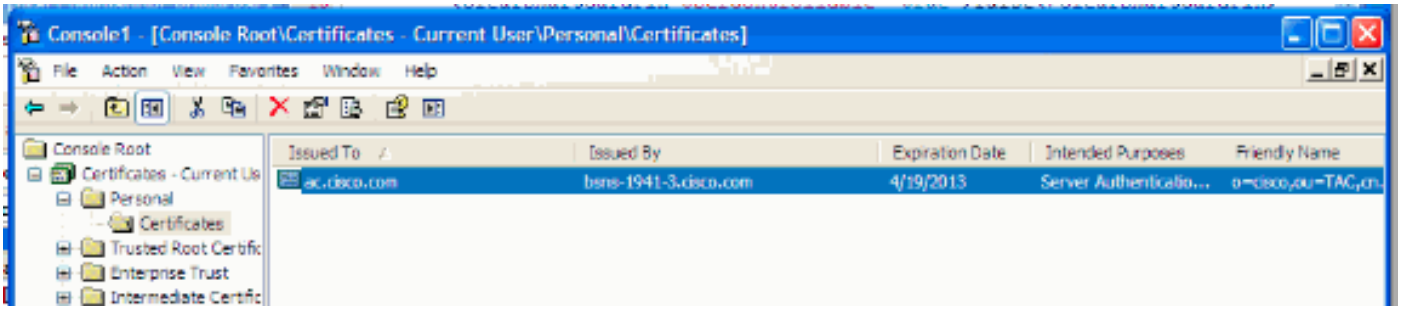
```
identity local dn
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

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
```

Client

Die Client-Konfiguration für eine erfolgreiche AnyConnect-Verbindung mit IKEv2 und Zertifikate besteht aus zwei Teilen.

Zertifikatsregistrierung

Wenn das Zertifikat ordnungsgemäß registriert ist, können Sie überprüfen, ob es sich im Automaten- oder im Privatspeicher befindet. Denken Sie daran, dass auch die Kundenzertifikate EKU erfordern.



AnyConnect-Profil

Das AnyConnect-Profil ist langwierig und sehr einfach.

Der entsprechende Teil ist zu definieren:

1. Host, mit dem Sie eine Verbindung herstellen
2. Protokolltyp
3. Authentifizierung bei Verbindung mit diesem Host

Wofür wird angewendet:

```
<ServerList>
<HostEntry>
<HostName>bsns-1941-4.cisco.com</HostName>
```

```
<PrimaryProtocol>IPsec
<StandardAuthenticationOnly>true
<AuthMethodDuringIKENegotiation>
IKE-RSA
</AuthMethodDuringIKENegotiation>
</StandardAuthenticationOnly>
</PrimaryProtocol>
</HostEntry>
</ServerList>
```

Im Anbindungsfeld von AnyConnect müssen Sie den vollständigen FQDN bereitstellen, den unter `<HostName>` angezeigten Wert.

Verbindungsüberprüfung

Einige Informationen werden aus Gründen der Kürze weggelassen.

```
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)
```

Verschlüsselungstechnologie der nächsten Generation

Die obige Konfiguration dient als Referenz, um eine minimale funktionierende Konfiguration anzuzeigen. Cisco empfiehlt, soweit möglich die Verschlüsselungstechnologie der nächsten Generation (NGC) zu verwenden.

Aktuelle Migrationsempfehlungen finden Sie hier:
http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Achten Sie bei der Auswahl der NGC-Konfiguration darauf, dass sowohl die Client-Software als auch die Headend-Hardware diese unterstützen. Die Router der ISR Generation 2 und ASR 1000 werden aufgrund ihrer Hardwareunterstützung für NGC als Headends empfohlen.

Auf der AnyConnect-Seite wird ab der Version AnyConnect 3.1 die Suite B-Algorithmus-Suite von NSA unterstützt.

Bekannte Vorbehalte und Probleme

- Denken Sie daran, dass diese Leitung auf Ihrem IOS-Headend konfiguriert ist: **kein crypto ikev2 http-url cert**. Der Fehler von IOS und AnyConnect, wenn dieser nicht konfiguriert ist, ist ziemlich irreführend.
- Die frühe IOS 15.2M&T-Software mit IKEv2-Sitzung wird möglicherweise nicht für die RSA-SIG-Authentifizierung verfügbar sein. Dies kann mit der Cisco Bug-ID CSCtx31294 zusammenhängen (nur registrierte Kunden). Stellen Sie sicher, dass Sie die neueste 15.2M- oder 15.2T-Software ausführen.
- In bestimmten Szenarien kann IOS möglicherweise nicht den richtigen Vertrauenspunkt für die Authentifizierung auswählen. Cisco ist sich des Problems bewusst und wird mit Version 15.2(3)T1 und Version 15.2(4)M1 behoben.
- Wenn AnyConnect eine ähnliche Meldung meldet:
  ```
  The client certificate's cryptographic service provider(CSP)
  does not support the sha512 algorithm
  ```

Anschließend müssen Sie sicherstellen, dass die Integritäts-/PRF-Einstellung in Ihren IKEv2-Vorschlägen mit den Einstellungen übereinstimmt, die Ihre Zertifikate verarbeiten können. Im obigen Konfigurationsbeispiel wird SHA-1 verwendet.

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems