Esempio di configurazione di AnyConnect a IOS Headend over IPsec con IKEv2 e certificati

Sommario

Introduzione

Questo documento offre informazioni su come ottenere una connessione protetta con IPsec da un dispositivo che esegue il client AnyConnect a un router Cisco IOS® con la sola autenticazione del certificato utilizzando il framework FlexVPN.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- FlexVPN
- AnyConnect

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

Headend

Il router Cisco IOS può essere qualsiasi router in grado di eseguire IKEv2, con almeno la versione 15.2 M&T. Tuttavia, è consigliabile utilizzare una versione più recente (vedere la sezione avvertenze note), se disponibile.

Cliente

AnyConnect 3.x

Autorità di certificazione

In questo esempio, l'Autorità di certificazione (CA) eseguirà la versione 15.2(3)T.

Èfondamentale utilizzare una delle versioni più recenti, in quanto è necessario supportare l'utilizzo chiavi esteso (EKU).

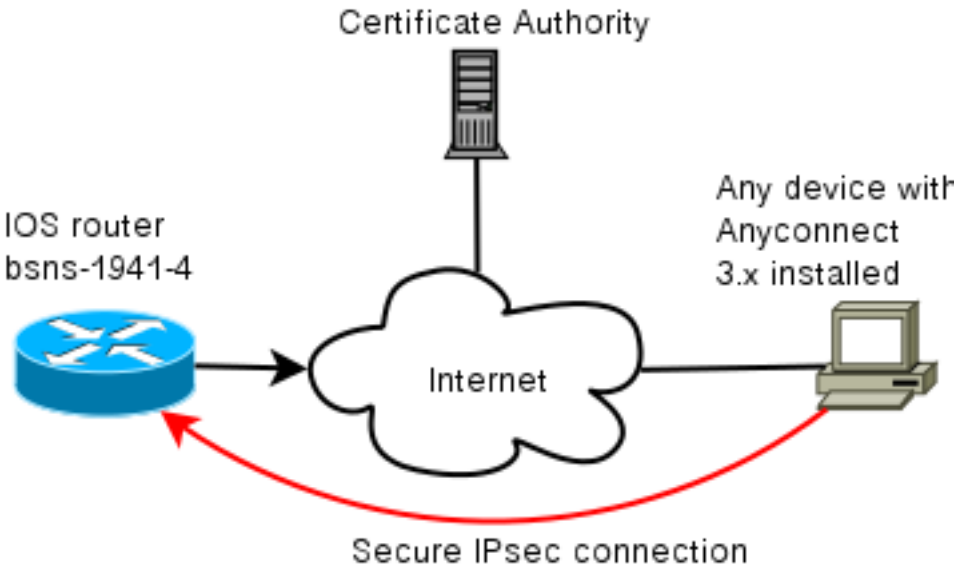
In questa distribuzione, il router IOS viene utilizzato come CA. Qualsiasi applicazione CA basata su standard in grado di utilizzare l'EKU dovrebbe tuttavia essere corretta.

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Configurazione

Topologia della rete



Autorità di certificazione (facoltativo)

Se si sceglie di utilizzarlo, il router IOS può fungere da CA.

Configurazione CA IOS

Ènecessario ricordare che il server CA deve inserire l'EKU corretto nei certificati client e server. In questo caso, per tutti i certificati sono stati impostati l'utilizzo chiavi avanzato server-auth e client-auth.

```
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
```

Verifica dell'impostazione dell'EKU corretto sul certificato

Notare che il bsns-1941-3 è il server CA, mentre il bsns-1941-4 è l'headend IPsec. Parti dell'output omesse per brevità.

```
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...)
```

Configurazione headend

La configurazione headend è composta da due parti: la parte PKI e il flexfield/IKEv2 effettivo.

Configurazione PKI

Si noti che viene utilizzato il CN bsns-1941-4.cisco.com. Questa opzione deve corrispondere a una voce DNS corretta e deve essere inclusa nel profilo AnyConnect in <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
```

Configurazione Crypto/IPsec

Si noti che l'impostazione PRF/integrità nella proposta **DEVE** corrispondere a quanto supportato dal certificato. Si tratta in genere di 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
```

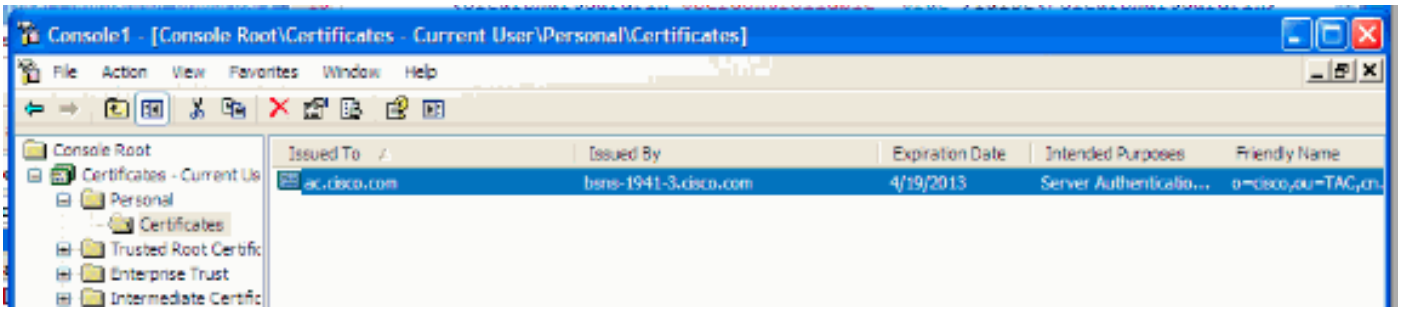
```
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

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
```

Cliente

La configurazione client per la riuscita della connessione AnyConnect con IKEv2 e i certificati è composta da due parti.

Registrazione certificato

Quando il certificato è stato registrato correttamente, è possibile verificare che sia presente nel computer o nell'archivio personale. Tenere presente che anche i certificati client devono disporre di EKU.



Profilo AnyConnect

Il profilo AnyConnect è lungo e molto semplice.

La parte pertinente è definire:

1. Host a cui si sta effettuando la connessione
2. Tipo di protocollo
3. Autenticazione da utilizzare per la connessione all'host

Utilizzo:

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

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

Nel campo della connessione di AnyConnect è necessario fornire l'FQDN completo, ossia il valore mostrato in `<HostName>`.

Verifica connessione

Alcune informazioni sono omesse per brevità.

```
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)
```

Crittografia di nuova generazione

La configurazione precedente viene fornita come riferimento per mostrare una configurazione di lavoro minima. Cisco consiglia di utilizzare la crittografia di nuova generazione (NGC), ove possibile.

Le raccomandazioni correnti per la migrazione sono disponibili all'indirizzo: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Quando si sceglie la configurazione NGC, accertarsi che sia il software client che l'hardware headend la supportino. Si consiglia l'uso di router ISR generazione 2 e ASR 1000 come headend perché supportano NGC.

Sul lato AnyConnect, a partire dalla versione 3.1 di AnyConnect, è supportata la suite di algoritmi Suite B dell'NSA.

Avvertenze e problemi noti

- Ricordarsi di configurare questa linea sull'headend IOS: **nessun certificato http-url crypto ikev2**. L'errore prodotto da IOS e AnyConnect quando non è configurato è piuttosto fuorviante.
- I primi software IOS 15.2 M e T con sessione IKEv2 potrebbero non essere disponibili per l'autenticazione RSA-SIG. Questa condizione può essere correlata all'ID bug Cisco CSCtx31294 (solo utenti registrati). Assicurarsi di eseguire il software 15.2M o 15.2T più recente.
- In alcuni scenari IOS potrebbe non essere in grado di selezionare il trust point corretto per l'autenticazione. Cisco è a conoscenza del problema e la sua risoluzione viene applicata alle versioni 15.2(3)T1 e 15.2(4)M1.
- Se AnyConnect segnala un messaggio simile a questo:
  ```
  The client certificate's cryptographic service provider(CSP)
  does not support the sha512 algorithm
  ```

Èquindi necessario verificare che l'impostazione di integrità/PRF nelle proposte IKEv2 corrisponda a quanto è in grado di gestire i certificati. Nell'esempio di configurazione precedente, viene utilizzato SHA-1.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems