AnyConnect al headend IOS sobre el IPSec con IKEv2 y el ejemplo de configuración de los Certificados

Contenido

Introducción

Este documento proporciona la información sobre cómo alcanzar una conexión protegida por IPsec de un dispositivo que funcione con al cliente de AnyConnect a un router del ® del Cisco IOS con solamente la autenticación certificada utilizando el marco de FlexVPN.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- FlexVPN
- AnyConnect

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

Headend

El router del Cisco IOS puede ser cualquier router capaz de ejecutar IKEv2, funcionando con por lo menos la versión 15.2 M&T. Sin embargo, usted debe utilizar una más nueva versión (véase la sección de las advertencias conocidas), si está disponible.

Cliente

Versión de AnyConnect 3.x

Certificate Authority

En este ejemplo, el Certificate Authority (CA) funcionará con la versión 15.2(3)T.

Es crucial que una de las más nuevas versiones está utilizado debido a la necesidad de soportar el uso dominante extendido (EKU).

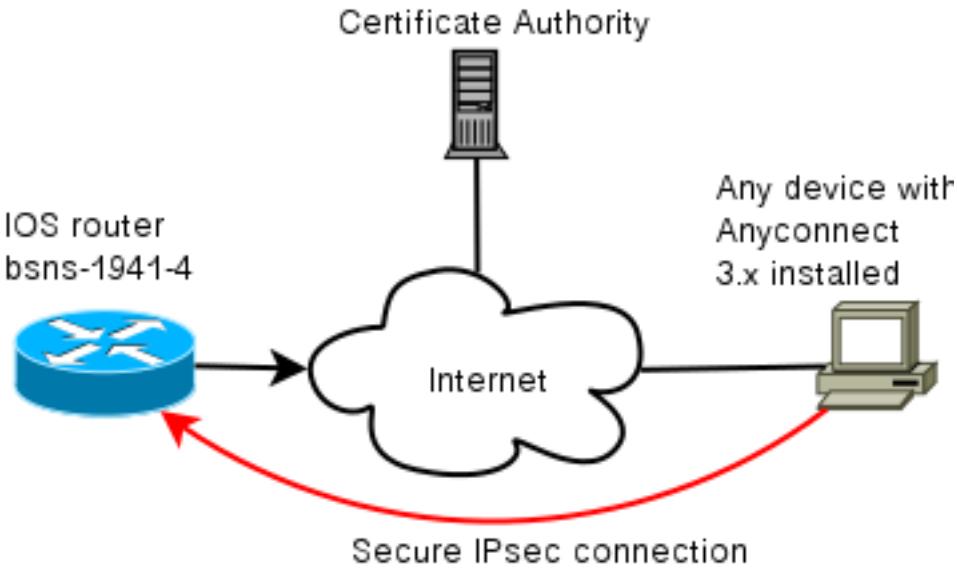
En este despliegue, utilizan al router IOS como CA. Sin embargo, cualquier aplicación basada en estándares de CA capaz de usar el EKU debe ser fina.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Configuración

Topología de red



Certificate Authority (opcional)

Si usted elige utilizarla, su router IOS puede actuar como CA.

Configuración IOS CA

Usted necesita recordar que el servidor de CA deba poner el EKU correcto en los Certificados de cliente y servidor. En este caso el servidor-auth y el EKU del cliente-auth fueron fijados para todos los Certificados.

```
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
```

Cómo verificar si está correcto el EKU fue fijado en el certificado

Observe que bsns-1941-3 es el servidor de CA mientras que bsns-1941-4 es el headend del IPSec. Salida de las partes de omitida para la brevedad.

```
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...)
```

Configuración del headend

La configuración del headend se comprende de dos porciones: la pieza PKI y el flex/IKEv2 real.

Configuración PKI

Usted notará que el CN de bsns-1941-4.cisco.com está utilizado. Esto necesita hacer juego una entrada DNS apropiada y necesita ser incluida en el perfil de AnyConnect bajo el <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
```

Crypto/configuración IPSec

Observe que su configuración PRF/integrity en la oferta NECESITA hacer juego lo que sus Soportes de certificado. Éste es típicamente 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
```

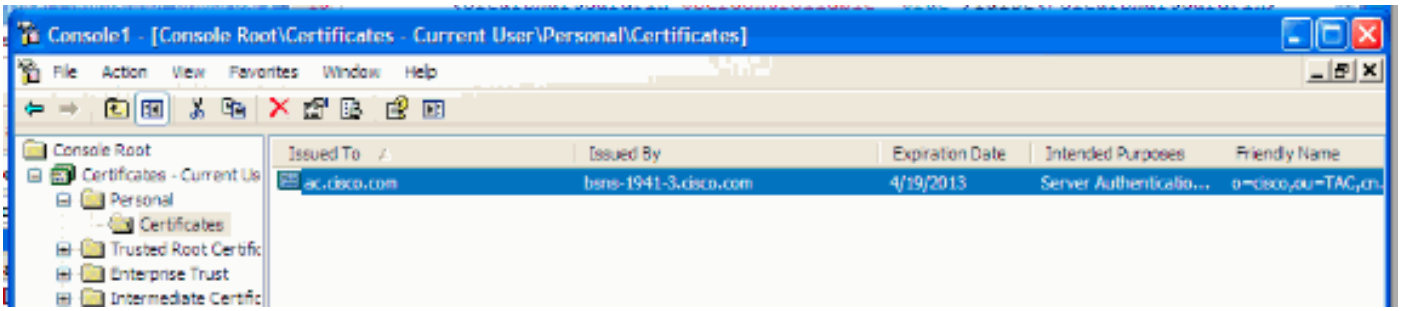
```
no crypto ikev2 http-url cert
crypto ipsec transform-set TRA esp-3des esp-sha-hmac

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 configuración del cliente para una conexión acertada de AnyConnect con IKEv2 y los Certificados consiste en dos porciones.

Inscripción del certificado

Cuando el certificado se alista correctamente, usted puede verificar que esté presente en la máquina o el almacén personal. Recuerde que los certificados del cliente también necesitan tener EKU.



Perfil de AnyConnect

El perfil de AnyConnect es muy largo y muy básico.

La parte pertinente es definir:

1. Host que usted está conectando con
2. Tipo de protocolo
3. Autenticación que se utilizará cuando está conectado con ese host

Se utiliza qué:

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

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

En el campo de la conexión de AnyConnect usted necesita proporcionar el FQDN lleno, que es el valor visto en el `<hostname>`.

Verificación de la conexión

Una cierta información se omite para la brevedad.

```
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)
```

Criptografía de la última generación

La configuración antedicha se proporciona para que la referencia muestre una configuración en funcionamiento mínima. Cisco recomienda usando la criptografía de la última generación (NGC) en lo posible.

Las recomendaciones actuales para la migración se pueden encontrar aquí: http://www.cisco.com/web/about/security/intelligence/nextgen_crypto.html

Al elegir la configuración NGC, aseegurese que software de cliente y soporte del hardware del headend él. Recomiendan la generación 2 ISR y los 1000 Router ASR como headends debido a su soporte del hardware para NGC.

En el lado de AnyConnect, a partir de la versión de AnyConnect 3.1, se soporta la habitación del algoritmo de la habitación B NSA.

Advertencias conocidas y problemas

- Recuerde tener esta línea configurada en su headend IOS: **ningún HTTP URL CERT crypto ikev2**. El error producido por el IOS y AnyConnect cuando esto no se configura es muy engañoso.
- El software temprano IOS 15.2M&T con la sesión IKEv2 no pudo subir para la autenticación RSA-SIG. Esto se puede relacionar con el Id. de bug Cisco CSCtx31294 (clientes registrados solamente). Aseegurese funcionar con el último 15.2M o software 15.2T.
- En ciertos escenarios el IOS no pudo poder escoger el trustpoint correcto para autenticar. Cisco es consciente del problema, y se repara a partir de las versiones 15.2(3)T1 y 15.2(4)M1.
- Si AnyConnect está señalando un mensaje similar a esto:
```
The client certificate's
cryptographic service provider(CSP)
does not support the sha512 algorithm
```

Entonces, usted necesita aseegurarse que la configuración integrity/PRF en su coincidencia de las ofertas IKEv2 qué sus Certificados pueden dirigir. En el ejemplo de configuración arriba, se utiliza el SHA-1.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems