Ejemplo de Configuración de AnyConnect to IOS Headend Over IPsec with IKEv2 and Certificates

Contenido

Introducción

Este documento proporciona información sobre cómo lograr una conexión protegida por IPSec desde un dispositivo que ejecuta el cliente AnyConnect a un router Cisco IOS® con sólo autenticación de certificado mediante el uso del marco FlexVPN.

Prerequisites

Requirements

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.

Encabezado

El router Cisco IOS puede ser cualquier router capaz de ejecutar IKEv2, ejecutando al menos la versión 15.2 M&T. Sin embargo, debe utilizar una versión más reciente (consulte la sección advertencias conocidas), si está disponible.

Cliente

Versión AnyConnect 3.x

Autoridad de certificados

En este ejemplo, la autoridad certificadora (CA) ejecutará la versión 15.2(3)T.

Es fundamental que se utilice una de las versiones más recientes debido a la necesidad de admitir el uso de clave extendida (EKU).

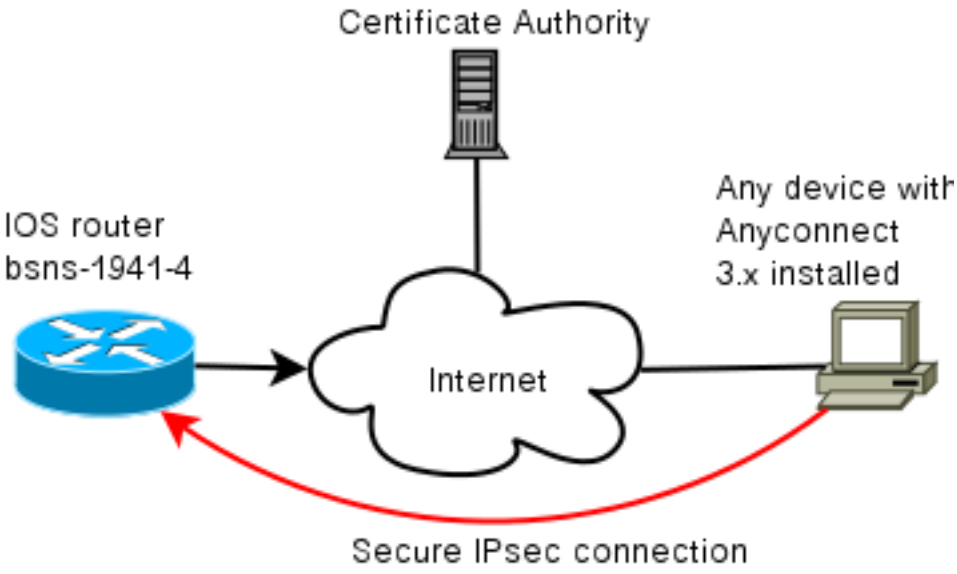
En esta implementación, el router IOS se utiliza como CA. Sin embargo, cualquier aplicación CA basada en estándares capaz de utilizar EKU debe estar bien.

Convenciones

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

Configuración

Topología de red



Autoridad certificadora (opcional)

Si decide utilizarla, el router IOS puede actuar como una CA.

configuración de CA del IOS

Debe recordar que el servidor de la CA debe poner la EKU correcta en los certificados de cliente y servidor. En este caso, se configuró EKU servidor-autenticación y cliente-autenticación 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 la EKU correcta se estableció en el certificado

Tenga en cuenta que bsns-1941-3 es el servidor de CA mientras que bsns-1941-4 es la cabecera IPsec. Partes de la salida omitidas 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 de cabecera

La configuración de cabecera consta de dos partes: la parte PKI y flex/IKEv2 real.

configuración PKI

Observará que se utiliza CN de bsns-1941-4.cisco.com. Esto debe coincidir con una entrada DNS adecuada y debe incluirse en el perfil de AnyConnect en <Nombre de host>.

```
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
```

Configuración de cifrado/IPSec

Tenga en cuenta que su configuración de PRF/integridad en la propuesta **NECESITA** coincidir con lo que su certificado admite. Esto suele ser 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
```

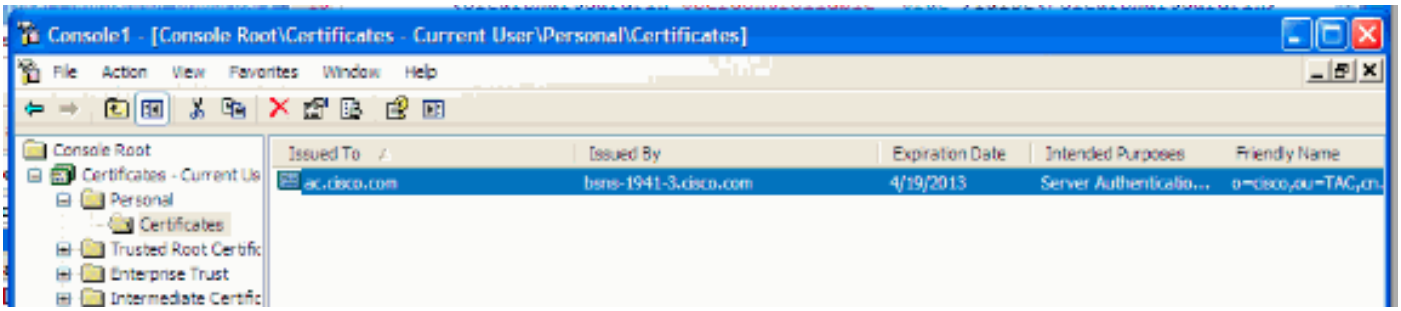
```
authentication remote rsa-sig
authentication local rsa-sig
pki trustpoint CISCO2
aaa authorization group cert list default AC
virtual-template 1

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 AnyConnect correcta con IKEv2 y los certificados consta de dos partes.

Inscripción de certificados

Cuando el certificado está correctamente inscrito, puede verificar que está presente en la máquina o en el almacén personal. Recuerde que los certificados de cliente también necesitan tener EKU.



perfil de AnyConnect

El perfil de AnyConnect es largo y muy básico.

La parte pertinente es definir:

1. Host al que se conecta
2. Tipo de protocolo
3. Autenticación que se utilizará cuando se conecte a ese host

Qué se utiliza:

```
<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 conexión de AnyConnect debe proporcionar el FQDN completo, que es el valor que se ve en `<HostName>`.

Verificación de la conexión

Se omite parte de la información por 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 última generación

La configuración anterior se proporciona como referencia para mostrar una configuración de funcionamiento mínima. Cisco recomienda utilizar la criptografía de última generación (NGC) siempre que sea 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 de NGC, asegúrese de que tanto el software del cliente como el hardware de cabecera lo admitan. Los routers ISR de segunda generación y ASR 1000 se recomiendan como cabeceras debido a su soporte de hardware para NGC.

En el lado de AnyConnect, a partir de la versión AnyConnect 3.1, se admite el conjunto de algoritmos Suite B de la NSA.

Advertencias y problemas conocidos

- Recuerde tener esta línea configurada en su cabecera IOS: **no crypto ikev2 http-url cert**. El error producido por IOS y AnyConnect cuando no se configura es bastante engañoso.
- Es posible que el software IOS 15.2M&T temprano con sesión IKEv2 no se active para la autenticación RSA-SIG. Esto puede estar relacionado con el ID de bug de Cisco CSCtx31294 (sólo clientes registrados) . Asegúrese de ejecutar el software 15.2M o 15.2T más reciente.
- En algunos escenarios, es posible que IOS no pueda elegir el punto de confianza correcto para autenticar. Cisco es consciente del problema y se ha corregido a partir de las versiones 15.2(3)T1 y 15.2(4)M1.
- Si AnyConnect está notificando un mensaje similar a este:
  ```
  The client certificate's cryptographic service provider(CSP)
  does not support the sha512 algorithm
  ```

A continuación, debe asegurarse de que la configuración de integridad/PRF de sus propuestas IKEv2 coincide con lo que pueden manejar sus certificados. En el ejemplo de configuración anterior, se utiliza SHA-1.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems