Configuración dinámica de FlexVPN con las listas de atribución locales AAA

Contenido

Introducción

Este ejemplo de configuración demuestra cómo utilizar la autenticación local, la lista de atribución de la autorización, y de las estadísticas (AAA) para realizar dinámico y potencialmente la configuración avanzada sin el uso del servidor externo del Remote Authentication Dial-In User Service (RADIUS).

Esto se desea en ciertos escenarios, especialmente cuando se requiere la instrumentación rápida o la prueba. Tales implementaciones son típicamente laboratorios del proof-of-concept, nueva prueba del despliegue, o troubleshooting.

La configuración dinámica es importante en el concentrador/el lado del eje de conexión donde las diversos directivas o atributos se deben aplicar en por usuario, por-cliente, base del por session.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa encendido, pero no se limita a, estas versiones de software y hardware. Esta lista no delinea los requerimientos mínimos, sino refleja el estado del dispositivo en la fase de prueba de esta característica.

Hardware

- La agregación mantiene al Routers (el ASR) - ASR 1001 - el "bsns-asr1001-4" llamado
- Generación 2 (ISR G2) del Routers de los Servicios integrados - 3925e - el "bsns-3925e-1" llamado
- Generación 2 (ISR G2) del Routers de los Servicios integrados - 3945e - el "bsns-3945e-1" llamado

Software

- Versión 3.8 del Cisco IOS XE - 15.3(1)S
- Software Release 15.2(4)M1 y 15.2(4)M2 de Cisco IOS®

Licencias

- Los routeres ASR hacen el **adventerprise** y las licencias de función del **IPSec** habilitar.
- El Routers ISR G2 hace las licencias de función **ipbasek9**, **securityk9**, y **hseck9** habilitar.

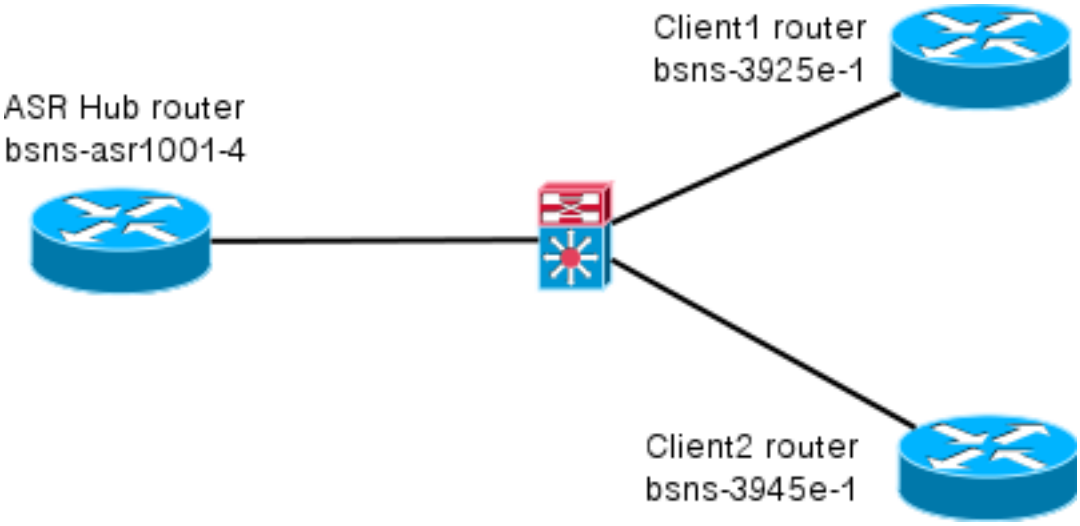
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

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

Topología

La topología usada en este ejercicio es básica. Utilizan a un router de eje de conexión (ASR) y a dos routeres radiales (ISR), que simulan a los clientes.



Configuraciones

Las configuraciones en este documento se piensan para mostrar una configuración básica, con los valores por defecto elegantes tanto cuanto sea posible. Para las Recomendaciones de Cisco en la criptografía, visite la página del cifrado de la última generación en cisco.com.

Configuración radial

Según lo mencionado previamente, la mayor parte de las acciones en esta documentación se realizan en el concentrador. La configuración radial está aquí para la referencia. En esta configuración, note que solamente el cambio es identidad entre el client1 y Client2 (visualizados en intrépido).

```
aaa new-model
aaa authorization network default local
aaa session-id common

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
crypto ikev2 profile Flex_IKEv2
 match identity remote address 0.0.0.0
 identity local email Client1@cisco.com authentication remote pre-share authentication local
pre-share keyring local Flex_key aaa authorization group psk list default default virtual-
template 1 crypto logging session crypto ipsec profile default set ikev2-profile Flex_IKEv2
interface Tunnel1 ip address negotiated ip mtu 1400 ip nhrp network-id 2 ip nhrp shortcut
virtual-template 1 ip nhrp redirect ip tcp adjust-mss 1360 tunnel source GigabitEthernet0/0
tunnel destination 172.25.1.1 tunnel path-mtu-discovery tunnel protection ipsec profile default
interface Virtual-Template1 type tunnel ip unnumbered Tunnel1 ip mtu 1400 ip nhrp network-id 2
ip nhrp shortcut virtual-template 1 ip nhrp redirect ip tcp adjust-mss 1360 tunnel path-mtu-
discovery tunnel protection ipsec profile default
```

Configuración del hub

La Configuración del hub se divide en dos porciones:

1. **La configuración de la conectividad básica**, que delinea la configuración necesitó para la conectividad básica.

2. **La configuración extendida**, que delinea los cambios de configuración necesitó para demostrar cómo un administrador puede utilizar la lista de atribución AAA para realizarse por usuario o los cambios de configuración del por session.

Configuración de conectividad básica

Esta configuración es para la referencia solamente y no se significa ser óptima, solamente funcional.

La limitación más grande de esta configuración es uso de la clave previamente compartida (PSK) como el método de autentificación. Cisco recomienda el uso de los Certificados siempre que sea aplicable.

```
aaa new-model
aaa authorization network default local

aaa session-id common
crypto ikev2 authorization policy default
 pool FlexSpokes
 route set interface

crypto ikev2 keyring Flex_key
 peer Spokes
 address 0.0.0.0 0.0.0.0
 pre-shared-key local cisco
 pre-shared-key remote cisco
 !!
 peer Client1
 identity email Client1@cisco.com
 pre-shared-key cisco
 !!
 peer Client2
 identity email Client2@cisco.com
 pre-shared-key cisco

crypto ikev2 profile Flex_IKEv2
 match fvrf any
 match identity remote address 0.0.0.0
 match identity remote email domain cisco.com
 authentication remote pre-share
 authentication local pre-share
 keyring local Flex_key
 aaa authorization group psk list default default
 virtual-template 1

no crypto ikev2 http-url cert

crypto logging session

crypto ipsec profile default
 set ikev2-profile Flex_IKEv2

interface Virtual-Template1 type tunnel
 vrf forwarding IVRF
 ip unnumbered Loopback100
 ip mtu 1400
 ip nhrp network-id 2
 ip nhrp redirect
 ip tcp adjust-mss 1360
 tunnel path-mtu-discovery
```

```
 tunnel vrf INTERNET
 tunnel protection ipsec profile default
```

Configuración extendida

Hay algunas cosas necesarias para asignar los atributos AAA a una sesión específica. Este ejemplo muestra el trabajo completo para el client1; entonces muestra cómo agregar otro cliente/usuario.

Configuración del hub extendida para el client1

1. Defina una lista de atribución AAA.`aaa attribute list Client1`
   `attribute type interface-config "ip mtu 1300" protocol ip`
   `attribute type interface-config "service-policy output TEST" protocol ip` **Nota:** Recuerde que la entidad asignada vía los atributos debe existir localmente. En este caso, el directiva-**mapa** fue configurado previamente.`policy-map TEST`
   `class class-default`
   `shape average 60000`
2. Asigne la lista de atribución AAA a una **directiva de la autorización.**`crypto ikev2 authorization policy` **`Client1`** `pool FlexSpokes aaa attribute list Client1 route set interface`
3. Asegúrese de que esta nueva directiva usada por los clientes que conectan. En este caso, extraiga la porción del **nombre de usuario de la** identidad enviada por los clientes. Los clientes deben utilizar una dirección de correo electrónico de ClientX@cisco.com (X es 1 o 2, dependiente en el cliente). **El mangler** parte la dirección de correo electrónico en la porción del nombre de usuario y del dominio y utiliza solamente uno de ellos (nombre de usuario en este caso) para elegir el nombre de la directiva de la autorización.`crypto ikev2 name-mangler GET_NAME`
   `email username`

   `crypto ikev2 profile Flex_IKEv2`
   `aaa authorization group psk list default name-mangler GET_NAME`Cuando el client1 es operativo, client2 puede ser relativamente fácil agregado.

Configuración del hub extendida para Client2

Asegure una directiva y a un conjunto aparte de atributos, si es necesario, existen.

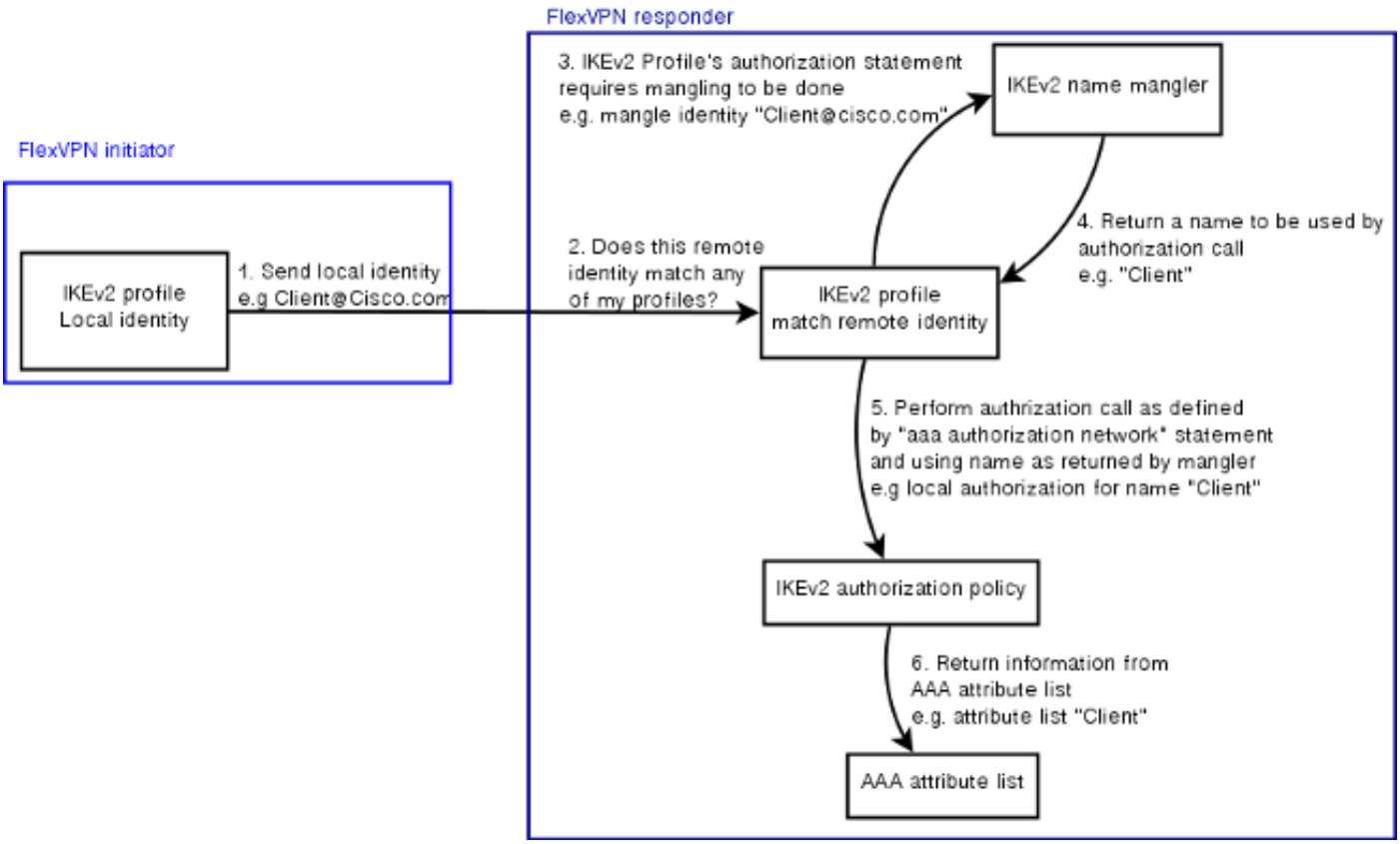
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

crypto ikev2 authorization policy Client2
 pool FlexSpokes
 aaa attribute list Client2
 route set interface
```

En este ejemplo, un Maximum Segment Size actualizado (MSS) que fija y una lista de acceso de entrada para actuar para este cliente es aplicados. Otras configuraciones pueden ser elegidas fácilmente. Una configuración típica es asignar el diversos ruteo virtual y expedición (VRF) para diversos clientes. Según lo mencionado anterior, cualquier entidad asignada a la lista de atribución, tal como lista de acceso 133 en este escenario, debe existir ya en la configuración.

Descripción de proceso

Esta figura delinea el orden de funcionamiento cuando la autorización AAA se procesa vía el perfil del intercambio de claves de Internet versión 2 (IKEv2) y contiene el específico de la información a este ejemplo de configuración.



Verificación

Esta sección muestra cómo verificar que las configuraciones asignadas previamente se han aplicado a los clientes.

Client1

Aquí están los comandos que verifican que se hayan aplicado las configuraciones de las unidades de transmisión máxima (MTU), así como la política de servicio.

```
bsns-asr1001-4#show cef int virtual-access 1 (...) Hardware idb is Virtual-Access1 Fast
switching type 14, interface type 21 IP CEF switching enabled IP CEF switching turbo vector IP
Null turbo vector VPN Forwarding table "IVRF" IP prefix lookup IPv4 mtrie 8-8-8-8 optimized
Tunnel VPN Forwarding table "INTERNET" (tableid 2) Input fast flags 0x0, Output fast flags
0x4000 ifindex 16(16) Slot unknown (4294967295) Slot unit 1 VC -1 IP MTU 1300 Real output
interface is GigabitEthernet0/0/0 bsns-asr1001-4#show policy-map interface virtual-access1
Virtual-Access1 Service-policy output: TEST Class-map: class-default (match-any) 5 packets, 620
bytes 5 minute offered rate 0000 bps, drop rate 0000 bps Match: any Queueing queue limit 64
packets (queue depth/total drops/no-buffer drops) 0/0/0 (pkts output/bytes output) 5/910 shape
(average) cir 60000, bc 240, be 240 target shape rate 60000
```

Client2

Aquí están los comandos que verifican que se hayan avanzado las configuraciones MSS y que la lista de acceso 133 también se ha aplicado como filtro de entrada en la interfaz de acceso virtual equivalente.

```
bsns-asr1001-4#show cef int virtual-access 2 Virtual-Access2 is up (if_number 18) Corresponding
hwidb fast_if_number 18 Corresponding hwidb firstsw->if_number 18 Internet address is 0.0.0.0/0
Unnumbered interface. Using address of Loopback100 (192.168.1.1) ICMP redirects are never sent
Per packet load-sharing is disabled IP unicast RPF check is disabled Input features: Access
List, TCP Adjust MSS (...) bsns-asr1001-4#show ip interface virtual-access2 Virtual-Access2 is
up, line protocol is up Interface is unnumbered. Using address of Loopback100 (192.168.1.1)
Broadcast address is 255.255.255.255 MTU is 1400 bytes Helper address is not set Directed
broadcast forwarding is disabled Outgoing access list is not set Inbound access list is 133,
default is not set (...)
```

Depurar

Hay dos bloques importantes a hacer el debug de. Esto es útil cuando usted necesita abrir un caso TAC y conseguir las cosas en la pista más rápidas.

Debug IKEv2

Comience con este comando debug importante:

```
debug crypto ikev2 [internal|packet]
```

Entonces ingrese estos comandos:

```
show crypto ikev2 sa show crypto ipsec sa peer a.b.c.d
```

Haga el debug de la asignación del atributo AAA

Si usted quisiera hacer el debug de la asignación AAA de los atributos, estos debugs pueden ser útiles.

```
debug aaa authorization
debug aaa attr
debug aaa proto local
```

Conclusión

Este documento demuestra cómo utilizar la lista de atribución AAA para permitir la flexibilidad agregada en las implementaciones de FlexVPN donde el servidor de RADIUS no pudo estar disponible o no se desea. La lista de atribución AAA ofrece las opciones de configuración agregadas en un por session, para cada grupo, si se requiere.

Información Relacionada

- FlexVPN y guía de configuración de la versión 2 del intercambio de claves de Internet, Cisco IOS Release 15M&T
- Servicios del usuario de acceso telefónico con autenticación remota (RADIUS)
- Solicitudes de Comentarios (RFC)
- Negociación IPSec/Protocolos IKE
- Soporte Técnico y Documentación - Cisco Systems