Configuración dinámica de FlexVPN con listas de atributos AAA locales

Contenido

Introducción

Este ejemplo de configuración muestra cómo utilizar la lista de atributos de autenticación, autorización y contabilidad (AAA) local para realizar una configuración dinámica y potencialmente avanzada sin el uso del servidor RADIUS (Servicio de usuario de acceso telefónico de autenticación remota) externo.

Esto se desea en determinados escenarios, especialmente cuando se requiere una implementación o prueba rápida. Tales implementaciones suelen ser laboratorios de prueba de concepto, nuevas pruebas de implementación o solución de problemas.

La configuración dinámica es importante en el lado del concentrador/concentrador, donde se deben aplicar diferentes políticas o atributos por usuario, por cliente y por sesión.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware, pero no se limita a ellas. Esta lista no describe los requisitos mínimos, pero refleja el estado del dispositivo durante la fase de prueba de esta función.

Hardware

- Routers de servicios de agregación (ASR) - ASR 1001 - llamados "bsns-asr1001-4"
- Routers de servicios integrados de segunda generación (ISR G2) - 3925e - llamados "bsns-3925e-1"
- Routers de servicios integrados de segunda generación (ISR G2) - 3945e - llamados "bsns-3945e-1"

Software

- Cisco IOS XE versión 3.8 - 15.3(1)S
- Software Cisco IOS® versión 15.2(4)M1 y 15.2(4)M2

Licencias

- Los routers ASR tienen habilitadas las licencias de funciones de **empresa** e **ipsec**.
- Los routers ISR G2 tienen habilitadas las licencias de funciones **ipbasek9**, **securityk9** y **hseck9**.

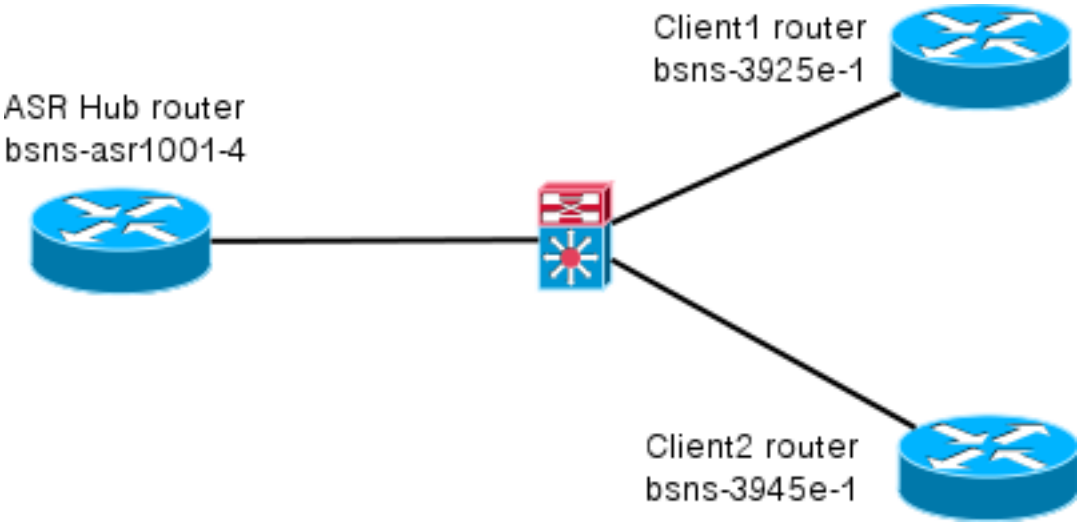
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Topología

La topología utilizada en este ejercicio es básica. Se utilizan un router hub (ASR) y dos routers spoke (ISR), lo que simula a los clientes.



Configuraciones

Las configuraciones de este documento están diseñadas para mostrar una configuración básica, con valores predeterminados inteligentes tanto como sea posible. Para obtener recomendaciones de Cisco sobre criptografía, visite la página Encriptación de última generación en cisco.com.

Configuración de Spoke

Como se mencionó anteriormente, la mayoría de las acciones de esta documentación se realizan en el hub. La configuración de spoke está aquí para referencia. En esta configuración, observe que sólo el cambio es la identidad entre Client1 y Client2 (mostrado en negrita).

```
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 partes:

1. **Configuración básica de conectividad**, que describe la configuración necesaria para la conectividad básica.
2. **Configuración ampliada**, que describe los cambios de configuración necesarios para demostrar cómo un administrador puede utilizar la lista de atributos AAA para realizar cambios de configuración por usuario o por sesión.

Configuración de conectividad básica

Esta configuración es sólo de referencia y no pretende ser óptima, sólo funcional.

La mayor limitación de esta configuración es el uso de clave previamente compartida (PSK) como método de autenticación. Cisco recomienda el uso de certificados cuando 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 ampliada

Hay algunas cosas necesarias para asignar atributos AAA a una sesión determinada. Este ejemplo muestra el trabajo completo para el cliente1; muestra cómo agregar otro cliente/usuario.

Configuración de concentrador extendido para cliente1

1. Defina una lista de atributos 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 a través de atributos debe existir localmente. En este caso, **policy-map** se configuró previamente.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. Asigne la lista de atributos AAA a una **política de autorización.**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. Asegúrese de que los clientes que se conectan utilizan esta nueva política. En este caso, extraiga la parte de **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, según el cliente). El **administrador** divide la dirección de correo electrónico en el nombre de usuario y la parte del dominio y utiliza sólo uno de ellos (nombre de usuario en este caso) para elegir el nombre de la política de 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 client1 está operativo, client2 se puede agregar relativamente fácil.

Configuración de concentrador extendido para el cliente 2

Asegúrese de que exista una política y un conjunto independiente de atributos, si es necesario.

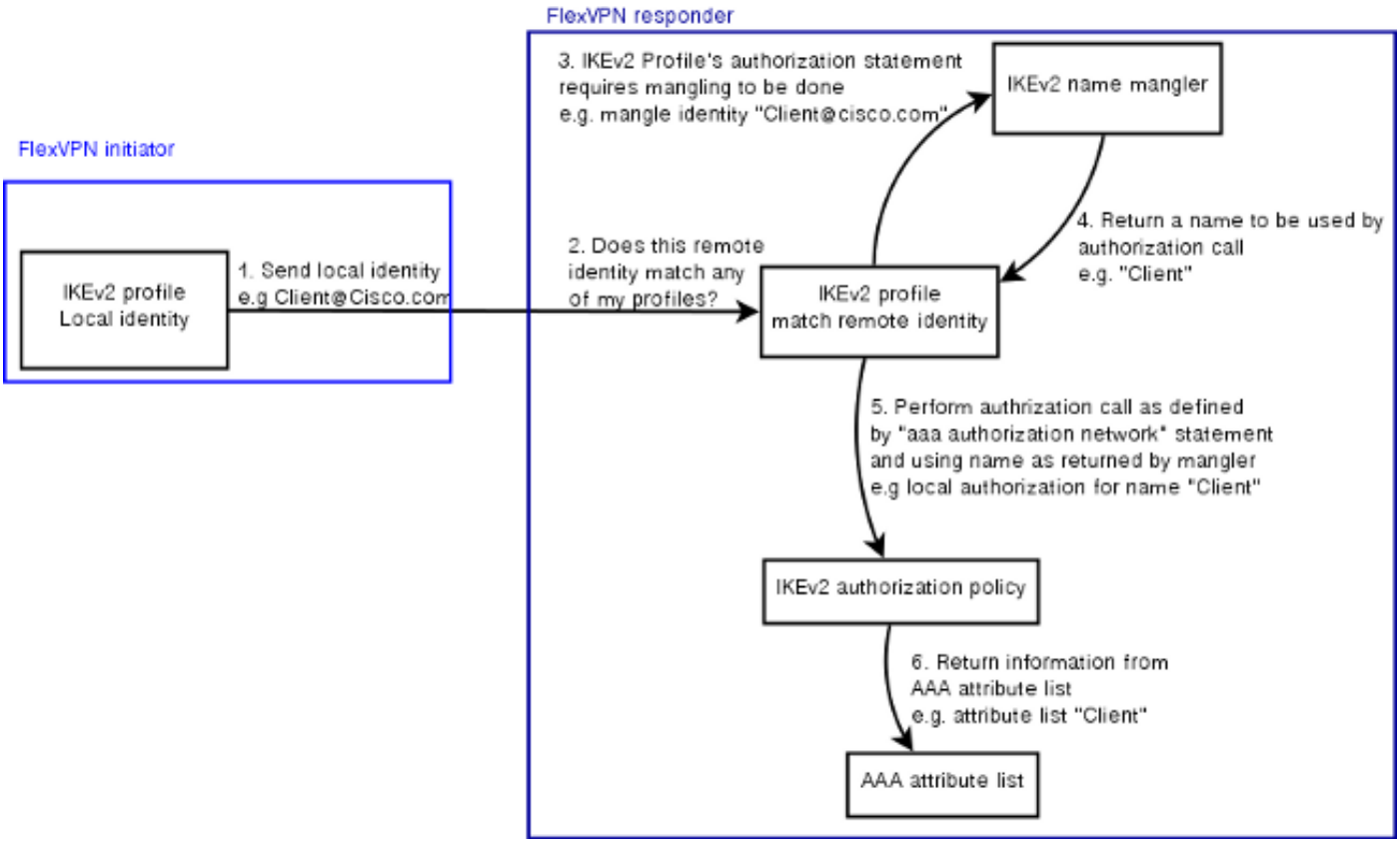
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

En este ejemplo, se aplica una configuración de tamaño máximo de segmento (MSS) actualizada y una lista de acceso entrante para funcionar para este cliente. Se pueden seleccionar fácilmente otros parámetros. Una configuración típica consiste en asignar diferentes tipos de routing y reenvío virtuales (VRF) para diferentes clientes. Como se mencionó anteriormente, cualquier entidad asignada a la lista de atributos, como access-list 133 en este escenario, ya debe existir en la configuración.

Descripción general del proceso

Esta figura describe el orden de funcionamiento cuando se procesa la autorización AAA a través del perfil de Intercambio de claves de Internet versión 2 (IKEv2) y contiene información específica de este ejemplo de configuración.



Verificación

Esta sección muestra cómo verificar que la configuración asignada previamente se haya aplicado a los clientes.

Cliente1

Estos son los comandos que verifican que se hayan aplicado la configuración 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
```

Cliente2

Estos son los comandos que verifican que la configuración de MSS se haya enviado y que la lista de acceso 133 también se haya aplicado como filtro entrante 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 principales para depurar. Esto es útil cuando necesita abrir un caso TAC y hacer que las cosas se encaucen más rápido.

Depurar IKEv2

Empiece con este comando debug principal:

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

Luego ingrese estos comandos:

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

Debug AAA Attribute Assignment

Si desea depurar la asignación AAA de atributos, estas depuraciones pueden resultar útiles.

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

Conclusión

Este documento muestra cómo utilizar la lista de atributos AAA para permitir mayor flexibilidad en implementaciones FlexVPN donde el servidor RADIUS podría no estar disponible o no ser deseado. La lista de atributos AAA ofrece opciones de configuración agregadas por sesión y por grupo, si es necesario.

Información Relacionada

- Guía de Configuración de FlexVPN e Internet Key Exchange Versión 2, Cisco IOS Release 15M&T
- Servicios de usuario de acceso telefónico de autenticación remota (RADIUS)
- Solicitudes de Comentarios (RFC)
- Negociación IPSec/Protocolos IKE

- Soporte Técnico y Documentación - Cisco Systems