Configuration dynamique FlexVPN avec listes d'attributs AAA locales

Contenu

Introduction

Cet exemple de configuration montre comment utiliser la liste d'attributs AAA (Authentication, Authorization, and Accounting) locale afin d'effectuer une configuration dynamique et potentiellement avancée sans utiliser le serveur RADIUS (Remote Authentication Dial-In User Service) externe.

Cela est souhaitable dans certains scénarios, en particulier lorsque le déploiement ou le test rapide est nécessaire. Ces déploiements sont généralement des travaux pratiques de validation de principe, de nouveaux tests de déploiement ou de dépannage.

La configuration dynamique est importante du côté concentrateur/concentrateur, où différentes politiques ou attributs doivent être appliqués par utilisateur, par client et par session.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur ces versions logicielles et matérielles, mais pas uniquement. Cette liste ne décrit pas les exigences minimales, mais reflète l'état du périphérique tout au long de la phase de test de cette fonctionnalité.

Matériel

- Routeurs de services d'agrégation (ASR) - ASR 1001 - appelé « bsns-asr1001-4 »
- Routeurs à services intégrés de 2e génération (ISR G2) - 3925e - appelés « bsns-3925e-1 »
- Routeurs à services intégrés de 2e génération (ISR G2) - 3945e - appelés « bsns-3945e-1 »

le logiciel Cisco IOS

- Cisco IOS XE version 3.8 - 15.3(1)S
- Logiciel Cisco IOS® versions 15.2(4)M1 et 15.2(4)M2

Licences

- Les licences de fonctionnalités **d'entreprise** et **ipsec** sont activées sur les routeurs ASR.
- Les licences de fonctionnalités **ipbasek9**, **securityk9** et **hseck9** sont activées sur les routeurs ISR G2.

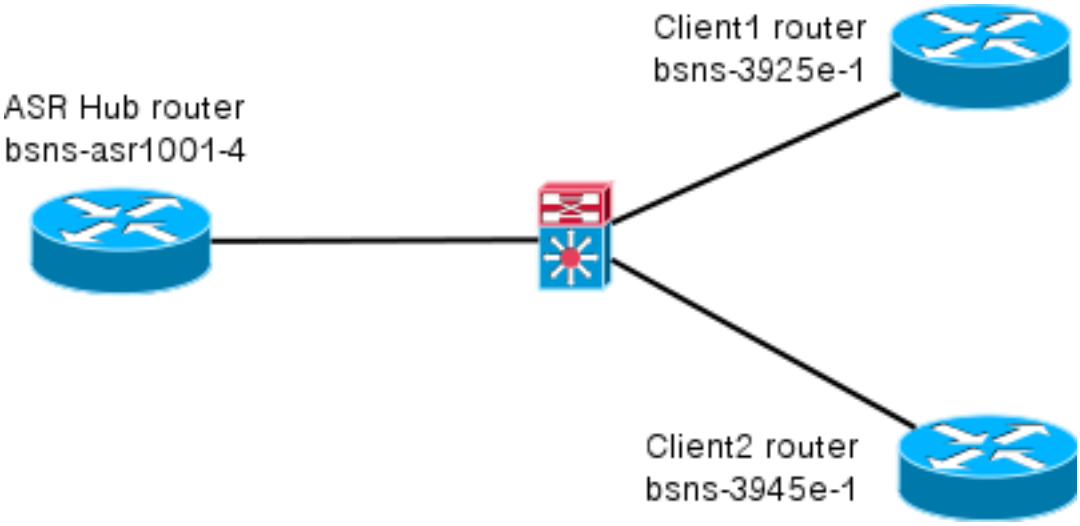
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Topologie

La topologie utilisée dans cet exercice est de base. Un routeur concentrateur (ASR) et deux routeurs en étoile (ISR) sont utilisés, ce qui simule les clients.



Configurations

Les configurations de ce document sont destinées à afficher une configuration de base, avec des valeurs par défaut intelligentes autant que possible. Pour obtenir des recommandations de Cisco sur la cryptographie, visitez la page Next Generation Encryption sur cisco.com.

Configuration du rayon

Comme indiqué précédemment, la plupart des actions de cette documentation sont exécutées sur le concentrateur. La configuration des rayons est ici à titre de référence. Dans cette configuration, notez que seule la modification est l'identité entre Client1 et Client2 (affichée en gras).

```
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
```

Configuration du concentrateur

La configuration du concentrateur est divisée en deux parties :

1. **Configuration de connectivité de base**, qui décrit la configuration requise pour la connectivité de base.
2. **Configuration étendue**, qui décrit les modifications de configuration nécessaires afin de démontrer comment un administrateur peut utiliser la liste d'attributs AAA pour effectuer des modifications de configuration par utilisateur ou par session.

Configuration de la connectivité de base

Cette configuration est réservée à la référence et n'est pas conçue pour être optimale, mais seulement fonctionnelle.

La plus grande limite de cette configuration est l'utilisation de la clé prépartagée (PSK) comme méthode d'authentification. Cisco recommande l'utilisation de certificats, le cas échéant.

```
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
```

Configuration étendue

Il y a quelques éléments nécessaires pour attribuer des attributs AAA à une session particulière. Cet exemple montre le travail complet pour le client 1 ; ensuite, il montre comment ajouter un autre client/utilisateur.

Configuration de concentrateur étendue pour Client1

1. Définissez une liste d'attributs AAA.
   ```
   aaa attribute list Client1
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Note : N'oubliez pas que l'entité affectée via des attributs doit exister localement. Dans ce cas, **policy-map** a été précédemment configuré.
   ```
   policy-map TEST
    class class-default
    shape average 60000
   ```
2. Affectez une liste d'attributs AAA à une **stratégie d'autorisation.**
   ```
   crypto ikev2 authorization policy Client1
    pool FlexSpokes
    aaa attribute list Client1
    route set interface
   ```
3. Assurez-vous que cette nouvelle stratégie est utilisée par les clients qui se connectent. Dans ce cas, extrayez la partie **nom d'utilisateur** de l'identité envoyée par les clients. Les clients doivent utiliser l'adresse e-mail ClientX@cisco.com (X est 1 ou 2, selon le client). Le **gestionnaire** divise l'adresse e-mail en nom d'utilisateur et en partie de domaine et n'utilise qu'un seul d'entre eux (nom d'utilisateur dans ce cas) pour choisir le nom de la stratégie d'autorisation.
   ```
   crypto ikev2 name-mangler GET_NAME
    email username
   ```

```
crypto ikev2 profile Flex_IKEv2
 aaa authorization group psk list default name-mangler GET_NAME
```

Lorsque le client1 est opérationnel, le client2 peut être ajouté relativement facilement.

Configuration de concentrateur étendue pour Client2

S'assurer qu'il existe une stratégie et un ensemble distinct d'attributs, le cas échéant.

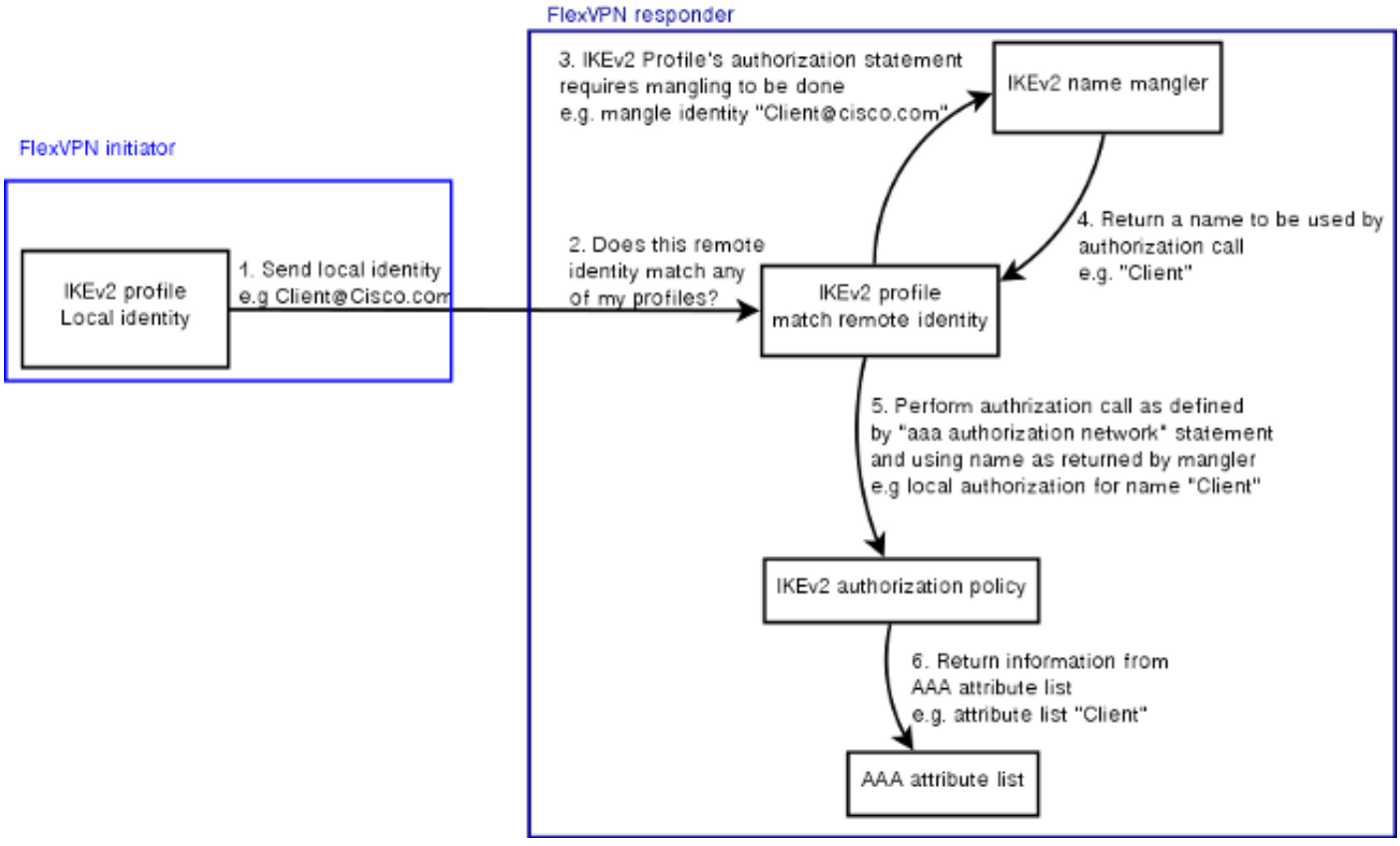
```
aaa attribute list Client2
 attribute type interface-config "ip tcp adjust-mss 1200" protocol ip
 attribute type interface-config "ip access-group 133 in" protocol ip

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

Dans cet exemple, un paramètre MSS (Maximum Segment Size) mis à jour et une liste d'accès entrante pour fonctionner pour ce client sont appliqués. D'autres paramètres peuvent être facilement choisis. Un paramètre type consiste à affecter différents VRF (Virtual Routing and Forwarding) à différents clients. Comme indiqué précédemment, toute entité affectée à la liste d'attributs, telle que access-list 133 dans ce scénario, doit déjà exister dans la configuration.

Présentation du processus

Cette figure décrit l'ordre de fonctionnement lorsque l'autorisation AAA est traitée via le profil Internet Key Exchange version 2 (IKEv2) et contient des informations spécifiques à cet exemple de configuration.



Vérification

Cette section montre comment vérifier que les paramètres précédemment attribués ont été appliqués aux clients.

Client1

Voici les commandes qui vérifient que les paramètres des unités de transmission maximale (MTU), ainsi que la stratégie de service ont été appliqués.

```
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

Voici les commandes qui vérifient que les paramètres MSS ont été poussés et que la liste d'accès 133 a également été appliquée en tant que filtre entrant sur l'interface d'accès virtuelle équivalente.

```
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
(...)
```

Déboguer

Il y a deux blocs principaux à déboguer. Cela est utile lorsque vous avez besoin d'ouvrir un dossier TAC et de faire avancer les choses plus rapidement.

Déboguer IKEv2

Commencez par cette commande de débogage principale :

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

Entrez ensuite les commandes suivantes :

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

Debug AAA Attribute Assignment

Si vous souhaitez déboguer l'affectation AAA des attributs, ces débogages peuvent être utiles.

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

Conclusion

Ce document explique comment utiliser la liste d'attributs AAA afin de permettre une plus grande flexibilité dans les déploiements FlexVPN où le serveur RADIUS n'est peut-être pas disponible ou n'est pas souhaité. La liste d'attributs AAA offre des options de configuration supplémentaires par session et par groupe, si nécessaire.

Informations connexes

- Guide de configuration FlexVPN et Internet Key Exchange version 2, Cisco IOS version 15M&T
- RADIUS (Remote Authentication Dial-In User Services)
- Demandes de commentaires (RFC)
- Négociation IPSec/Protocoles IKE

- Support et documentation techniques - Cisco Systems