Configuration dynamique de FlexVPN avec les listes locales d'aaa attribute

Contenu

Introduction

Cet exemple de configuration explique comment employer la liste d'authentification locale, d'attribut d'autorisation, et de comptabilité (AAA) afin d'exécuter dynamique et potentiellement la configuration avancée sans utilisation de serveur externe de Service RADIUS (Remote Authentication Dial-In User Service).

Ceci est désiré dans certains scénarios, particulièrement quand le déploiement ou le test rapide est exigé. De tels déploiements sont typiquement des laboratoires de preuve-de-concept, nouveau test de déploiement, ou dépannage.

La configuration dynamique est importante du concentrateur/du côté concentrateur où différents stratégies ou attributs devraient être appliqués sur un par-utilisateur, par-client, base de par-session.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations dans ce document sont basées en fonction, mais pas limitées à, ces logiciel et versions de matériel. Cette liste ne trace pas les grandes lignes des conditions requises minimum, mais reflète l'état du périphérique tout au long de la phase de test de cette caractéristique.

Matériel

- L'agrégation entretient les Routeurs (l'ASR) - ASR 1001 - "bsns-asr1001-4" appelé
- Génération 2 (ISR G2) d'Integrated Services Router - 3925e - "bsns-3925e-1" appelé
- Génération 2 (ISR G2) d'Integrated Services Router - 3945e - "bsns-3945e-1" appelé

Logiciel

- Version 3.8 de Cisco IOS XE - 15.3(1)S
- Versions de logiciel 15.2(4)M1 et 15.2(4)M2 de Cisco IOS®

Permis

- Des Routeurs ASR font activer les permis de caractéristique d'**adventerprise** et d'**ipsec**.
- Des Routeurs d'ISR G2 font activer des permis de la caractéristique **ipbasek9**, **securityk9**, et **hseck9**.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

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, qui simulent des clients.

Configurations

Les configurations dans ce document sont destinées pour afficher une installation de base, avec des par défaut intelligents autant que possible. Pour des recommandations de Cisco concernant le chiffrement, visitez la page de cryptage de nouvelle génération sur cisco.com.

Configuration du rayon

Comme mentionné précédemment, la plupart des actions dans cette documentation sont

exécutées sur le hub. La configuration en étoile est ici pour la référence. Dans cette configuration, notez que la seule modification est identité entre Client1 et Client2 (affichés 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 de hub est divisée en deux parts :

1. **La configuration de base de Connectivité**, qui trace les grandes lignes de la configuration a eu besoin pour la Connectivité de base.
2. **La configuration étendue**, qui trace les grandes lignes des modifications de configuration a dû afin d'expliquer comment un administrateur peut employer l'aaa attribute list pour exécuter des modifications de configuration de par-utilisateur ou de par-session.

Configuration de base de Connectivité

Cette configuration est pour la référence seulement et n'est pas censée être optimale, seulement fonctionnel.

La plus grande limite de cette configuration est utilisation de la clé pré-partagée (PSK) comme méthode d'authentification. Cisco recommande l'utilisation des Certificats toutes les fois qu'applicable.

```
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 choses requises pour assigner des attributs d'AAA à une session particulière. Cet exemple affiche le travail complet pour client1 ; alors il affiche comment ajouter un client/utilisateur différents.

Configuration étendue de hub pour Client1

1. Définissez un aaa attribute list.`aaa attribute list Client1`
   ```
    attribute type interface-config "ip mtu 1300" protocol ip
    attribute type interface-config "service-policy output TEST" protocol ip
   ```
   Remarque: Souvenez-vous que l'entité assignée par l'intermédiaire des attributs doit exister localement. Dans ce cas, le **policy-map** a été précédemment configuré.`policy-map TEST`
   ```
    class class-default
    shape average 60000
   ```
2. Assignez l'aaa attribute list 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 utilisée par les clients qui se connectent. Dans ce cas, extrayez la partie de **nom d'utilisateur de l'**identité envoyée par les clients. Les clients devraient utiliser une adresse e-mail de ClientX@cisco.com (X est 1 ou 2, dépendant du client). **Le mangler** coupe l'adresse e-mail en partie de nom d'utilisateur et de domaine et emploie seulement un 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
```
Quand client1 est opérationnel, client2 peut être relativement facile ajouté.

Configuration étendue de hub pour Client2

Assurez une stratégie et un ensemble distinct d'attributs, si nécessaire, existez.

```
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, une configuration maximum mise à jour de la taille de segment (MSS) et une liste d'accès en entrée à fonctionner pour ce client est appliquée. D'autres configurations peuvent être facilement choisies. Une configuration typique est d'assigner le routage et l'expédition virtuels différents (VRF) pour différents clients. Comme cité précédemment, n'importe quelle entité assignée à la liste d'attribut, telle que la liste d'accès 133 dans ce scénario, doit déjà exister dans la configuration.

Aperçu de processus

Cette figure trace les grandes lignes de la commande de l'exécution quand l'autorisation d'AAA est traitée par l'intermédiaire du profil de la version 2 d'échange de clés Internet (IKE) (IKEv2) et contient la particularité de l'information à cet exemple de configuration.

Vérification

Cette section affiche comment vérifier que les configurations précédemment assignées ont été appliquées aux clients.

Client1

Voici les commandes qui vérifient que les configurations maximum d'unités de transmission (MTU), aussi bien que la stratégie de service ont été appliquées.

```
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 configurations MSS ont été poussées et que la liste d'accès 133 a été également appliquée comme filtre en entrée 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 (...)
```

Debug

Il y a deux blocs importants à mettre au point. C'est utile quand vous devez ouvrir une valise TAC et obtenir des choses sur la piste plus vite.

Debug IKEv2

Commencez par cette principale commande de débogage :

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

Sélectionnez alors ces commandes :

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

Affectation d'attribut de debug aaa

Si vous voudriez au debug aaa l'attribution des attributs, ceux-ci met au point peuvent être utiles.

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

Conclusion

Ce document explique comment employer l'aaa attribute list afin de permettre la flexibilité accrue dans des déploiements de FlexVPN où le serveur de RAYON ne pourrait pas être disponible ou n'est pas désiré. L'aaa attribute list offre des options de configuration ajoutées sur une par-session, base de par-groupe, si on l'exige.

Informations connexes

- FlexVPN et guide de configuration de version 2 d'échange de clés Internet (IKE), version de Cisco IOS 15M&T
- Remote Authentication Dial-In User Service (RAYON)
- Demandes de commentaires (RFC)
- Négociation IPSec/Protocoles IKE
- Support et documentation techniques - Cisco Systems