Configuration VPN site à site sur ASA 9.x à contexte multiple reçoit un message d'erreur

Contenu

Introduction

Ce document décrit comment dépanner le message d'erreur, « Le nombre maximal de tunnels autorisé a été atteint », lorsque vous configurez un VPN de site à site sur l'ASA 9.x.

Conditions préalables

Components Used

Les informations de ce document sont basées sur le logiciel ASA version 9.0 et ultérieure. Cette version a introduit la configuration VPN de site à site en mode de contexte multiple.

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

Lorsque vous essayez d'activer plusieurs tunnels VPN de site à site sur l'ASA, il échoue et génère le message syslog « Le nombre maximal de tunnels autorisé a été atteint ».

Le message syslog spécifique est le suivant :

```
%ASA-4-751019: Local:<LocalAddr> Remote:<RemoteAddr> Username:<username> Failed to obtain a
```

<licenseType> license.

- <LocalAddr> : adresse locale pour cette tentative de connexion
- <RemoteAddr> : adresse d'homologue distante pour cette tentative de connexion
- <username> : nom d'utilisateur pour la tentative de connexion par homologue
- <licenseType> : type de licence dépassé (autre VPN ou AnyConnect Premium/Essentials)

Informations générales

Le journal indique qu'une création de session a échoué car la limite de licence maximale pour les tunnels VPN a été dépassée, ce qui entraîne l'échec de l'initialisation ou de la réponse à une demande de tunnel.

La mise en oeuvre du VPN en mode multiple nécessite la division du total des licences VPN disponibles entre les contextes configurés. L'administrateur ASA peut configurer le nombre de licences attribuées à chaque contexte.

Par défaut, aucune licence de tunnel VPN n'est allouée aux contextes et l'allocation du type de licence doit être effectuée manuellement par l'administrateur.

Action recommandée

Assurez-vous que suffisamment de licences sont disponibles pour tous les utilisateurs autorisés et/ou obtenez plus de licences pour autoriser les connexions rejetées. Pour le multicontexte, allouez davantage de licences au contexte qui a signalé l'échec, si possible.

Solution

La division des licences entre les contextes est effectuée par l'augmentation du gestionnaire de ressources avec une ressource 'VPN other' qui gère la division du pool de licences 'Other VPN' utilisé pour le VPN de site à site entre les contextes configurés.

L'interface de ligne de commande limit-resource ci-dessous autorise cette configuration dans le mode 'class' de la ressource.

```
Limit-resource vpn [burst] other <value> | <value>%
```

Où, <valeur> : 1- Limite de licence de plate-forme ou 1 à 100 % des licences installées.

Pour les rafales, la plage est comprise entre 1 et les licences non attribuées ou entre 1 et 100 % des licences non attribuées.
Par défaut : 0; aucune ressource VPN n'est allouée à une classe.

Pour affecter un contexte à 10 % des licences installées, vous devez définir une classe de ressources. Ensuite, appliquez la classe aux contextes dont vous avez besoin pour obtenir cette ressource dans la configuration du contexte système.

```
ciscoasa(config)# class vpn
```

```
ciscoasa(config-class)# limit-resource vpn other 10%
```

Afin d'attribuer un contexte de 250 homologues VPN des licences installées, vous devez définir une ressource 'class'. Ensuite, appliquez la classe aux contextes que vous préférez être en mesure d'obtenir cette ressource dans la configuration du contexte système.

```
ciscoasa(config)# class vpn
ciscoasa(config-class)# limit-resource vpn other 250
```

Pour appliquer la classe ci-dessus « vpn » à un contexte appelé « administrateur », procédez comme suit :

1. Modifiez/changez le contexte système et appliquez le VPN de classe pour le contexte « administrateur ». Cela ne peut être fait que dans le contexte du système.
2. Ci-dessous se trouve l'extrait de configuration pour allouer la classe « vpn » au contexte « administrateur ».

   ```
   ciscoasa(config)# context administrator
   ciscoasa(config-ctx)# member vpn
   ```

Informations connexes

- Guides de référence des pare-feu de nouvelle génération Cisco ASA 5500
- Guides de configuration des pare-feu de nouvelle génération de la gamme Cisco ASA 5500
- Support et documentation techniques - Cisco Systems