La configuration du VPN de site à site sur le plusieurs contexte ASA 9.x reçoit le message d'erreur

Contenu

Introduction

Ce document décrit comment dépanner le message d'erreur, « le compte maximum de tunnel permis a été atteint », quand vous configurez un site à site VPN sur les plusieurs appliances de sécurité adaptable de contexte (ASA) 9.x.

Conditions préalables

Composants utilisés

Les informations dans ce document sont basées sur la version de logiciel 9.0 ASA et plus tard. Cette configuration du VPN de site à site introduite par version dans le mode de contexte multiple.

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 vivant, assurez-vous que vous comprenez l'impact potentiel de n'importe quelle commande.

Problème

Quand vous tentez d'évoquer de plusieurs tunnels VPN de site à site sur l'ASA, elle échoue et génère le message de Syslog « que le compte maximum de tunnel permis a été atteint ».

Le message spécifique de Syslog est ci-dessous :

```
%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 distante de pair pour cette tentative de connexion
- **<username>** - Nom d'utilisateur pour le pair tentant la connexion
- **<licenseType>** - Type de licence qui a été dépassé (l'autre premium VPN ou d'AnyConnect/essentiel)

Informations générales

Le log indique qu'une création de session a manqué parce que la limite maximum de permis pour des tunnels VPN a été dépassée qui entraîne une panne à l'initié ou répond à une demande de tunnel.

L'implémentation du VPN en multiple-mode exige la division de tous les permis disponibles VPN parmi les contextes configurés. L'administrateur ASA peut configurer combien de permis chaque contexte est alloué.

Par défaut, aucun permis de tunnel VPN n'est alloué aux contextes, et l'allocation du type de licence doit être faite manuellement par l'administrateur.

Action recommandée

Assurez qu'assez de permis sont disponibles pour tous les utilisateurs permis et/ou obtenez plus de permis de permettre les connexions rejetées. Pour le multi-contexte, allouez plus de permis au contexte qui a signalé la panne, si possible.

Solution

La division des permis parmi les contextes est faite par l'augmentation du gestionnaire de ressources avec « VPN une autre » ressource qui gère la division du groupe de permis « autre VPN » utilisé pour le site à site VPN parmi les contextes configurés.

Le limit-resource CLI ci-dessous permet cette configuration mode des classes dans ressource le « .

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

Là où, plage de **<value>** : 1 limite de permis de plate-forme ou 1-100% de permis installés.

Pour des rafales, la plage est 1 aux permis non affectés ou 1-100% de permis non affectés.
Par défaut : 0 ; aucune ressource VPN n'est allouée à une classe.

Afin d'assigner un contexte à 10% des permis installés, vous devez définir une classe de ressource. Ensuite, appliquez la classe aux contextes des lesquels vous avez besoin pour pouvoir obtenir cette ressource dans la configuration de contexte de système.

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

Afin d'assigner un contexte de 250 homologues VPN des permis installés, vous devez classes définir ressource des « . Ensuite, appliquez la classe aux contextes que vous préférez pouvoir obtenir cette ressource dans la configuration de contexte de système.

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

Afin d'appliquer la classe ci-dessus « vpn » à un contexte a appelé le « administrateur », suivent ces étapes :

1. La modification/basculement au contexte de système et appliquent la classe VPN pour le contexte « administrateur ». Ceci a pu être fait seulement dans le contexte de système.
2. Est ci-dessous 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 de Pare-feu de nouvelle génération de gamme de Cisco ASA 5500
- Guides de configuration de Pare-feu de nouvelle génération de gamme de Cisco ASA 5500
- Support et documentation techniques - Cisco Systems