Contenu

Question

Pourquoi l'agent de Teamviewer ne fonctionne-t-il pas quand l'authentification est activée sur la sécurité Web Aplliance (WSA) de Cisco ?

Environnement

Appliance de sécurité Web de Cisco (WSA), et toute version d'AsyncOS.

Symptômes

Les temps d'agent de Teamviewer et les entrées d'expositions d'accesslogs qui contiennent 401 ou 407 erreurs indiquant la « authentification de proxy ont exigé ».

Les agents de Teamviewer ne fonctionnent pas avec l'authentification - signification quand les demandes WSA de l'authentification de l'application de TeamViewer, l'application peuvent ne pas fournir les qualifications de domaine. Ainsi il est nécessaire de l'exclure de l'authentification.

L'exemption d'authentification est exigée si WSA est configuré pour utiliser des **Témoins** comme substituts dans les identités (**GUI > gestionnaire > identités de sécurité Web**).

Si des identités sont configurées aux substituts d'**adresse IP**, alors les étapes ci-dessous ne peuvent être exigées parce que les qualifications du client sont cachées pendant une période égale **pour substituer le délai d'attente** (par défaut = 1 heure) une fois qu'elles accèdent à tous sites Web utilisant leur navigateur.

- **Remarque:** En mode explicite (utilisant le fichier ou les paramètres de proxy du navigateur PAC), assurez-vous s'il vous plaît que l'**application les mêmes configurations de remplacement à l'**option **en avant explicite de demandes** est vérifiée
- Nous pouvons encore employer les étapes ci-dessous pour sauter l'authentification si nous voyons par intermittence 401s/407s dans des logs d'accès tout en accédant à Teamviewer.

Pour configurer l'exemption d'authentification pour Teamviewer, suivez s'il vous plaît ces étapes :

Étape 1 : Créez une catégorie URL de coutume

L'agent de Teamviewer se connecte à différents serveurs avec différentes adresses IP, ainsi il est nécessaire d'installer quelques expressions régulières.

1. Naviguez vers le **Web GUI > gestionnaire de sécurité Web > des catégories faites sur commande URL**.
2. Cliquez sur le bouton **fait sur commande de catégorie d'ajouter…**.
3. Choisissez un nom de catégorie.
4. Dans les sites mettez en place, entrez dans ce qui suit : **.teamviewer.com, dyngate.com**.
5. Le clic **a avancé** et dans les expressions régulières mettez en place, ajoutez ce qui suit :
   vacarme \ .aspx
   dout \ .aspx
6. Soumettez et commettez vos modifications.

Étape 2 : Ajoutez une nouvelle identité

1. Naviguez vers le **Web GUI > gestionnaire > identités de sécurité Web**.
2. Cliquez sur le bouton d'**identité d'ajouter…**.
3. Créez l'identité sans l'**authentification**.
4. Cliquez sur le menu déroulant **avancé** et puis n'en cliquez sur l'**aucun** lien **sélectionné** à la droite des catégories URL.
5. Ajoutez la **catégorie** de création récente **URL de coutume** (voir s'il vous plaît ci-dessus) à l'identité en sélectionnant la ligne correcte.
6. Soumettez et commettez vos modifications.

Étape 3 : Ajoutez la nouvelle identité à une stratégie d'Access

Il y a deux possibilités pour faire ceci ; vous pouvez utiliser une stratégie existante d'Access ou créer un neuf.

Contournement pour l'usage d'une stratégie existante d'Access

1. Naviguez vers le **Web GUI > gestionnaire de sécurité Web > stratégies d'Access.**
2. Pour le nom de stratégie d'Access où on doit permettre l'URL de coutume, cliquez sur le lien sous la colonne de **catégories URL**.

3. Cliquez sur **[incluez] le** lien sur la catégorie faite sur commande de création récente, et placez l'action **de laisser** ou **surveiller**.

4. Soumettez et commettez vos modifications.

Contournement pour l'usage d'une nouvelle stratégie d'Access

1. Naviguez vers le **Web GUI > gestionnaire de sécurité Web > stratégies d'Access**.

2. Cliquez sur en fonction le bouton de **stratégie d'ajouter**….

3. Choisissez un ***<Policy Name>***.

4. Cliquez sur en fonction la liste déroulante d'**identités et d'utilisateurs** et choisissez l'identité de création récente.

5. Soumettez et commettez vos modifications.