Contenu

Introduction

Si vous vous connectez dans un serveur distant utilisant Remote Desktop Protocol (la RDP), et le nom d'utilisateur distant est différent que votre utilisateur, des évolutions des systèmes de FireSIGHT l'adresse IP de l'utilisateur qui est associé avec votre adresse IP au centre de Gestion de FireSIGHT. Il entraîne le changement des autorisations pour l'utilisateur par rapport aux règles de contrôle d'accès. Vous noterez que l'utilisateur incorrect est associé avec le poste de travail. Ce document fournit une solution pour cette question.

Conditions préalables

Cisco recommande que vous ayez la connaissance sur le système de FireSIGHT et l'agent d'utilisateur.

> Remarque: 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.

Cause principale

Cette question se produit en raison de la manière Microsoft Directory(AD) qu'actif se connecte la RDP les tentatives d'authentification à la protection windows ouvre une session le contrôleur de domaine. L'AD se connecte la tentative d'authentification pour la session RDP contre l'adresse IP d'origine d'hôte plutôt que le point final RDP que vous connectez à. Si vous vous connectez dans le serveur distant avec un compte utilisateur différent, ceci changera l'utilisateur associé avec l'adresse IP d'origine de votre poste de travail.

Vérification

Pour vérifier ceci est ce qui se produit, vous peut vérifier que l'adresse IP de l'événement de connexion de votre poste de travail d'origine et le serveur distant RDP ont la même adresse IP.

Pour trouver ces événements, vous devrez suivre les étapes ci-dessous :

Étape 1 : Déterminez le contrôleur de domaine contre lequel vous hébergez authentifie :

Exécutez la commande suivante :

Exemple de sortie :

La ligne qui commence le « C.C : » soyez le contrôleur de nom du domaine et la ligne que les débuts « adressent : » l'adresse IP.

Étape 2 : Utilisant la RDP le log dans le contrôleur de domaine l'a identifié dans l'étape 1

Étape 3 : Allez au **début > à l'Administrative Tools > Event Viewer**.

Étape 4 : Effectuez un zoom avant à **Windows se connecte > Sécurité**.

Étape 5 : Le filtre pour l'adresse IP de votre poste de travail en cliquant sur le log en cours de filtre, en cliquant sur l'onglet XML, et en cliquant sur éditent la requête.

Étape 6 : Écrivez la requête suivante XML, substituant votre adresse IP au <ip address>

Étape 7 : Cliquez sur en fonction l'**événement de connexion** et cliquez sur en fonction l'onglet de **détails**.

Un exemple de sortie :

Terminez-vous ces mêmes étapes après qu'ouvrir une session par l'intermédiaire de la RDP et de vous note que vous recevrez un autre événement de connexion (ID 4624 d'événement) avec la même adresse IP qu'affichée par la ligne suivante des données XML d'événement de connexion de la connexion d'origine :

Solution

Pour atténuer cette question, si vous utilisez l'agent d'utilisateur 2.1 ou en haut, vous pouvez exclure tous les comptes que vous allez le faire
utilise principalement pour la RDP dans la configuration d'agent d'utilisateur.

Étape 1 : Connectez-vous dans l'hôte d'agent d'utilisateur.

Étape 2 : Lancez l'interface utilisateur d'agent d'utilisateur.

Étape 3 : Cliquez sur en fonction l'onglet **exclu de noms d'utilisateur**.

Étape 4 : Écrivez tous les noms d'utilisateur que vous souhaitez exclure.

Étape 5 : Cliquez sur **Save**.

Les utilisateurs présentés dans cette liste ne génèrent pas des événements de connexion au centre de Gestion de FireSIGHT et ne doivent pas être
associé aux adresses IP.