Usinez les avantages de restriction d'Access - et - des inconvénients

Contenu

Introduction

Ce document décrit un problème rencontré avec la restriction d'Access d'ordinateur (MARS), et fournit une solution au problème.

Avec la croissance des périphériques possédés par personnel, il est plus important que jamais que les administrateurs système fournissent une manière de limiter l'accès à certaines parties du réseau aux ressources possédées par d'entreprise seulement. Le problème décrit dans des soucis de ce document comment identifier sécurisé ces sujets de préoccupation et les authentifier sans interruptions à la Connectivité d'utilisateur.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance du 802.1x afin de comprendre entièrement ce document. Ce document suppose la connaissance de l'authentification de 802.1x d'utilisateur, et met en valeur les problèmes et les avantages attaché à l'utilisation de MARS, et plus généralement, authentification de machine.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

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.

Problème

De MARS les tentatives fondamentalement de résoudre un problème courant inhérent à la plupart du courant et des méthodes populaires de Protocole EAP (Extensible Authentication Protocol), à savoir ces authentification de machine et authentification de l'utilisateur sont des processus distincts et indépendants.

L'authentification de l'utilisateur est une méthode d'authentification de 802.1x qui est bien connue à la plupart des administrateurs système. L'idée est que des qualifications (nom d'utilisateur/mot de passe) sont données à chaque utilisateur, et que l'ensemble de qualifications représente une personne physique (il peut être aussi bien partagé entre plusieurs personnes). Par conséquent, un utilisateur peut ouvrir une session n'importe où dedans du réseau avec ces qualifications.

Une authentification de machine est techniquement identique, mais l'utilisateur n'est pas typiquement incité à entrer dans les qualifications (ou le certificat) ; l'ordinateur ou l'ordinateur fait cela seule. Ceci exige de l'ordinateur d'avoir déjà des qualifications enregistrées. Le nom d'utilisateur envoyé est **host/<MyPCHostname>**, à condition que votre ordinateur ait le <MyPCHostname > réglé comme adresse Internet. En d'autres termes, il envoie le **serveur** suivi de votre adresse Internet.

Bien que pas directement associé à Microsoft Windows et au Répertoire actif de Cisco, ce processus est rendu plus facilement si l'ordinateur est joint au Répertoire actif parce que l'adresse Internet d'ordinateur est ajoutée à la base de données de domaine, et des qualifications sont négociées (et a renouvelé tous les 30 jours par défaut) et enregistrées sur l'ordinateur. Ceci signifie que l'authentification de machine est possible de n'importe quel type d'appareil, mais elle est rendue beaucoup plus facilement et d'une manière transparente si l'ordinateur est joint au Répertoire actif, et les qualifications restent masquées de l'utilisateur.

MARS comme solution

Il est facile de dire que la solution est pour le système de contrôle d'accès de Cisco (ACS) ou Logiciel Cisco Identity Services Engine (ISE) pour finir MARS, mais il y a des avantages et des inconvénients à considérer avant que ceci soit mis en application. Comment implémenter ceci mieux est décrit dans des guides utilisateurs ACS ou ISE, ainsi ce document décrit simplement si considérer lui, et quelques barrages de route possibles.

Les avantages

MARS a été inventé parce que l'utilisateur et les authentifications de machine sont totalement distincts. Par conséquent, le serveur de RADIUS ne peut pas imposer une vérification où les utilisateurs doivent ouvrir une session des périphériques de la société. Avec MARS, le serveur de RADIUS (ACS ou ISE, du Cisco-side) impose, pour une authentification de l'utilisateur donnée, qu'il doit y a une authentification de machine valide pendant les heures X (en général 8 heures, mais pendant ceci est configurable) qui précèdent l'authentification de l'utilisateur pour le même point final.

Par conséquent, une authentification de machine réussit si les qualifications d'ordinateur sont connues par le serveur de RADIUS, typiquement si l'ordinateur est joint au domaine, et le serveur de RADIUS vérifie ceci avec une connexion au domaine. Il est entièrement jusqu'à l'administrateur

réseau pour déterminer si une authentification de machine réussie fournit l'accès complet au réseau, ou seulement à un accès restreint ; typiquement, ceci ouvre au moins la connexion entre le client et le Répertoire actif de sorte que le client puisse exécuter des actions telles que le renouvellement des objets de stratégie de groupe de mot de passe utilisateur ou de téléchargement (GPO).

Si une authentification de l'utilisateur provient un périphérique où une authentification de machine ne s'est pas produite dans les couples précédents des heures, alors l'utilisateur est refusé, même si l'utilisateur est normalement valide.

On accorde seulement l'accès complet à un utilisateur si l'authentification est valide et terminée d'un point final où une authentification de machine s'est produite dans les couples passés des heures.

Les inconvénients

Cette section décrit les inconvénients de l'utilisation de MARS.

MARS et suppliant de Microsoft Windows

L'idée derrière MARS est celle pour qu'une authentification de l'utilisateur réussisse, doit non seulement que l'utilisateur ont les qualifications valides, mais une nécessité réussie d'authentification de machine sont enregistré de ce client aussi bien. S'il y a n'importe quel problème avec le ce, l'utilisateur ne peut pas authentifier. La question qui surgit est que cette caractéristique peut parfois par distraction lock-out un client légitime, qui force le client pour redémarrer afin de regagner l'accès au réseau.

Microsoft Windows exécute l'authentification de machine seulement au temps de démarrage (quand l'écran de connexion apparaît) ; dès que l'utilisateur écrira les identifiants utilisateurs, une authentification de l'utilisateur est exécutée. En outre, si l'utilisateur se ferme une session (des retours à l'écran de connexion), une nouvelle authentification de machine est exécutée.

Voici un exemple de scénario qui affiche pourquoi MARS pose parfois des problèmes :

L'utilisateur X a travaillé toute la journée sur son ordinateur portable, qui a été connecté par l'intermédiaire d'une connexion Sans fil. Finalement, il ferme simplement l'ordinateur portable et les feuilles fonctionnent. Ceci place l'ordinateur portable dans l'hibernation. Le next day, il revient dans le bureau et ouvre son ordinateur portable. Maintenant, il ne peut pas établir une connexion Sans fil.

Quand Microsoft Windows hiberne, il prend un instantané du système dans son état actuel, qui inclut le contexte de qui a été ouvert une session. Du jour au lendemain, l'entrée Mars-cachée pour l'ordinateur portable d'utilisateur expire et est purgée. Cependant, quand l'ordinateur portable est mis sous tension, il n'exécute pas une authentification de machine. Il entre à la place directement dans une authentification de l'utilisateur, puisqu'était ce ce que l'hibernation a enregistré. La seule manière de résoudre ceci est de se connecter l'utilisateur hors fonction, ou de redémarrer son ordinateur.

Bien que MARS soit une bonne caractéristique, il a le potentiel d'entraîner l'interruption du réseau. Il est difficile dépanner ces interruptions jusqu'à ce que vous comprenniez que la manière MARS fonctionne ; quand vous implémentez MARS, il est important d'instruire les utilisateurs au sujet de la façon arrêter correctement des ordinateurs et se fermer une session de chaque ordinateur à la

fin de chaque jour.

MARS et divers serveurs de RADIUS

Il est commun pour avoir plusieurs serveurs de RADIUS dans le réseau pour l'Équilibrage de charge et les raisons de redondance. Cependant, non tous les serveurs de RADIUS prennent en charge un cache partagé de session de MARS. Seulement versions 5.4 et ultérieures ACS, et synchronisation de cache de MARS de support de version 2.2 et ultérieures ISE entre les Noeuds. Avant ces versions, il n'est pas possible d'exécuter une authentification de machine contre un serveur ACS/ISE, et d'exécuter une authentification de l'utilisateur contre des autres, car ils ne correspondent pas les uns avec les autres.

MARS et commutation de Câbler-radio

Le cache de MARS de beaucoup de serveurs de RADIUS se fonde sur l'adresse MAC. C'est simplement une table avec l'adresse MAC des ordinateurs portables et l'horodateur de leur dernière authentification de machine réussie. De cette façon, le serveur peut savoir si le client était ordinateur authentifié pendant les dernières heures X.

Cependant, que se produit si vous démarrez votre ordinateur portable avec une connexion câblée (et font-elles donc une authentification de machine de votre MAC de câble) et puis commutez à la radio au cours de la journée ? Le serveur de RADIUS n'a aucun moyen de corréler votre adresse MAC Sans fil avec votre adresse MAC de câble et de savoir que vous étiez ordinateur authentifié pendant les heures passées X. La seule manière est de fermer une session et avoir l'attitude de Microsoft Windows une autre authentification de machine par l'intermédiaire de la radio.

Solution

Parmi beaucoup d'autres caractéristiques, le Cisco AnyConnect a l'avantage des profils préconfigurés qui ordinateur et authentification de l'utilisateur de déclencheur. Cependant, les mêmes limites que vues avec le suppliant de Microsoft Windows sont produites, quant à l'authentification de machine se produisant seulement quand vous vous fermez une session ou redémarrez.

En outre, avec des versions 3.1 et ultérieures d'AnyConnect, il est possible d'exécuter l'EAP-FAST avec l'Eap-enchaînement. C'est fondamentalement une authentification simple, où vous envoyez deux paires de qualifications, du nom d'utilisateur/mot de passe d'ordinateur et du nom d'utilisateur/mot de passe d'utilisateur, en même temps. ISE, alors, vérifie plus facilement que chacun des deux sont réussis. Sans le cache utilisé et aucun besoin de récupérer une session précédente, ceci présente la grande fiabilité.

Quand le PC démarre, AnyConnect envoie une authentification de machine seulement, parce qu'aucune informations utilisateur n'est disponible. Cependant, sur l'ouverture de session utilisateur, AnyConnect envoie les credentails d'ordinateur et d'utilisateur simultanément. En outre, si vous devenez déconnecté ou débranchez/replug le câble, l'ordinateur et des identifiants utilisateurs sont de nouveau introduits une authentification simple d'EAP-FAST, qui diffère des versions antérieures d'AnyConnect sans Eap-enchaînement.

EAP-TEAP est la meilleure solution à long terme car il est fait particulièrement pour prendre en charge ces le type d'authentifications, mais EAP-TEAP n'est toujours pas pris en charge dans le suppliant indigène des beaucoup SYSTÈME D'EXPLOITATION en date de ce jour