Avantages et inconvénients des restrictions d'accès aux machines

Contenu

Introduction

Ce document décrit un problème rencontré avec la restriction d'accès à la machine (MAR) et fournit une solution au problème.

Avec la croissance des périphériques personnels, il est plus important que jamais pour les administrateurs système de fournir un moyen de limiter l'accès à certaines parties du réseau aux ressources appartenant à l'entreprise uniquement. Le problème décrit dans ce document concerne la manière d'identifier en toute sécurité ces zones de préoccupation et de les authentifier sans perturber la connectivité des utilisateurs.

Conditions préalables

Conditions requises

Cisco vous recommande de connaître la norme 802.1x afin de bien comprendre ce document. Ce document prend en compte la familiarité avec l'authentification 802.1x de l'utilisateur et met en évidence les problèmes et les avantages liés à l'utilisation de MAR, et plus généralement, à l'authentification par machine.

Components Used

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

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. If your network is live, make sure that you understand the potential impact of any command.

Problème

MAR tente essentiellement de résoudre un problème commun inhérent à la plupart des méthodes EAP (Extensible Authentication Protocol) courantes et populaires, à savoir que l'authentification de la machine et l'authentification de l'utilisateur sont des processus distincts et indépendants.

L'authentification des utilisateurs est une méthode d'authentification 802.1x qui est familière à la plupart des administrateurs système. L'idée est que les informations d'identification (nom d'utilisateur/mot de passe) sont données à chaque utilisateur et que cet ensemble d'informations d'identification représente une personne physique (il peut également être partagé entre plusieurs personnes). Par conséquent, un utilisateur peut se connecter à partir de n'importe quel emplacement du réseau avec ces informations d'identification.

L'authentification d'une machine est techniquement la même, mais l'utilisateur n'est généralement pas invité à entrer les informations d'identification (ou le certificat) ; l'ordinateur ou la machine le fait tout seul. Cela nécessite que l'ordinateur dispose déjà d'informations d'identification stockées. Le nom d'utilisateur envoyé est **host/<MyPCHostname>**, à condition que **<MyPCHostname>** soit défini comme nom d'hôte sur votre machine. En d'autres termes, il envoie **l'hôte/**suivi de votre nom d'hôte.

Bien qu'il ne soit pas directement lié à Microsoft Windows et à Cisco Active Directory, ce processus est rendu plus facilement si l'ordinateur est joint à Active Directory parce que le nom d'hôte de l'ordinateur est ajouté à la base de données de domaine et que les informations d'identification sont négociées (et renouvelées tous les 30 jours par défaut) et stockées sur l'ordinateur. Cela signifie que l'authentification de la machine est possible à partir de n'importe quel type de périphérique, mais elle est rendue beaucoup plus facilement et de manière plus transparente si la machine est jointe à Active Directory et que les informations d'identification restent masquées de l'utilisateur.

La solution MAR

Il est facile de dire que la solution est que Cisco Access Control System (ACS) ou Cisco Identity Services Engine (ISE) complètent la fonction MAR, mais il y a des avantages et des inconvénients à prendre en compte avant de mettre en oeuvre cette fonction. La meilleure description de la mise en oeuvre de cette solution est fournie dans les guides d'utilisation ACS ou ISE. Par conséquent, ce document décrit simplement s'il convient de l'envisager ou non, ainsi que quelques obstacles éventuels.

Les avantages

MAR a été inventé parce que les authentifications des utilisateurs et des machines sont totalement distinctes. Par conséquent, le serveur RADIUS ne peut pas appliquer une vérification lorsque les utilisateurs doivent se connecter à partir de périphériques appartenant à l'entreprise. Avec MAR, le serveur RADIUS (ACS ou ISE, côté Cisco) impose, pour une authentification utilisateur donnée, qu'il doit y avoir une authentification machine valide dans les X heures (généralement 8 heures, mais configurable) qui précèdent l'authentification utilisateur pour le même terminal.

Par conséquent, l'authentification d'une machine réussit si les informations d'identification de la machine sont connues du serveur RADIUS, généralement si la machine est jointe au domaine, et le serveur RADIUS le vérifie avec une connexion au domaine. Il appartient entièrement à

l'administrateur réseau de déterminer si une authentification de machine réussie fournit un accès complet au réseau, ou seulement un accès limité ; généralement, cela ouvre au moins la connexion entre le client et Active Directory afin que le client puisse effectuer des actions telles que le renouvellement du mot de passe utilisateur ou le téléchargement d'objets de stratégie de groupe (GPO).

Si l'authentification d'un utilisateur provient d'un périphérique où l'authentification d'une machine n'a pas eu lieu au cours des deux dernières heures, l'utilisateur est refusé, même si l'utilisateur est normalement valide.

L'accès complet n'est accordé à un utilisateur que si l'authentification est valide et terminée à partir d'un point de terminaison où une authentification de machine s'est produite au cours des dernières heures.

Les Cons

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

MRA et Microsoft Windows Supplicator

L'idée derrière MAR est que pour qu'une authentification utilisateur réussisse, non seulement cet utilisateur doit avoir des informations d'identification valides, mais une authentification de machine réussie doit également être enregistrée à partir de ce client. En cas de problème, l'utilisateur ne peut pas s'authentifier. Le problème qui se pose est que cette fonctionnalité peut parfois verrouiller par inadvertance un client légitime, ce qui force le client à redémarrer afin de récupérer l'accès au réseau.

Microsoft Windows n'effectue l'authentification de l'ordinateur qu'au démarrage (lorsque l'écran de connexion apparaît); dès que l'utilisateur entre les informations d'identification de l'utilisateur, une authentification de l'utilisateur est effectuée. En outre, si l'utilisateur se déconnecte (retourne à l'écran de connexion), une nouvelle authentification de l'ordinateur est effectuée.

Voici un exemple de scénario qui montre pourquoi MAR cause parfois des problèmes :

L'utilisateur X travaillait toute la journée sur son ordinateur portable, qui était connecté via une connexion sans fil. En fin de compte, il ferme simplement l'ordinateur portable et laisse le travail. L'ordinateur portable est alors mis en veille prolongée. Le lendemain, il revient au bureau et ouvre son ordinateur portable. Maintenant, il ne peut pas établir de connexion sans fil.

Lorsque Microsoft Windows est mis en veille prolongée, il prend un instantané du système dans son état actuel, qui inclut le contexte de qui a été connecté. De nuit, l'entrée MAR mise en cache pour l'ordinateur portable utilisateur expire et est purgée. Cependant, lorsque l'ordinateur portable est sous tension, il n'effectue pas d'authentification de machine. Il va directement dans une authentification utilisateur, puisque c'est ce que l'hibernation a enregistré. La seule façon de résoudre ce problème est de déconnecter l'utilisateur, ou de redémarrer son ordinateur.

Bien que la fonction MAR soit une bonne fonctionnalité, elle peut entraîner des perturbations du réseau. Ces interruptions sont difficiles à dépanner tant que vous ne comprenez pas le fonctionnement de MAR ; lorsque vous mettez en oeuvre MAR, il est important d'informer les utilisateurs finaux sur la façon d'arrêter correctement les ordinateurs et de se déconnecter de chaque machine à la fin de chaque jour.

MAR et divers serveurs RADIUS

Il est courant d'avoir plusieurs serveurs RADIUS dans le réseau à des fins d'équilibrage de charge et de redondance. Cependant, tous les serveurs RADIUS ne prennent pas en charge un cache de session MAR partagé. Seules les versions ACS 5.4 et ultérieures, et ISE version 2.3 et ultérieures prennent en charge la synchronisation du cache MAR entre les noeuds. Avant ces versions, il n'est pas possible d'effectuer une authentification de machine sur un serveur ACS/ISE et d'effectuer une authentification d'utilisateur sur un autre, car ils ne correspondent pas entre eux.

Commutation MAR et sans fil

Le cache MAR de nombreux serveurs RADIUS repose sur l'adresse MAC. Il s'agit simplement d'une table avec l'adresse MAC des ordinateurs portables et l'horodatage de leur dernière authentification de machine réussie. De cette manière, le serveur peut savoir si le client a été authentifié par ordinateur au cours des X dernières heures.

Cependant, que se passe-t-il si vous démarrez votre ordinateur portable avec une connexion câblée (et par conséquent, faites une authentification de machine à partir de votre MAC câblée), puis passez à la technologie sans fil pendant la journée ? Le serveur RADIUS n'a aucun moyen de corréler votre adresse MAC sans fil avec votre adresse MAC câblée et de savoir que vous avez été authentifié par ordinateur au cours des X dernières heures. La seule façon est de se déconnecter et de demander à Microsoft Windows de procéder à une autre authentification de machine via le sans fil.

Solution

Parmi de nombreuses autres fonctionnalités, Cisco AnyConnect présente l'avantage de profils préconfigurés qui déclenchent l'authentification des machines et des utilisateurs. Cependant, les mêmes limitations que celles observées avec Microsoft Windows supplicant sont rencontrées, en ce qui concerne l'authentification de l'ordinateur qui se produit uniquement lorsque vous vous déconnectez ou redémarrez.

En outre, avec AnyConnect versions 3.1 et ultérieures, il est possible d'exécuter EAP-FAST avec le chaînage EAP. Il s'agit essentiellement d'une authentification unique, dans laquelle vous envoyez deux paires d'informations d'identification, le nom d'utilisateur/mot de passe de la machine et le nom d'utilisateur/mot de passe de l'utilisateur, en même temps. ISE vérifie alors plus facilement que les deux sont efficaces. Sans cache utilisé et sans besoin de récupérer une session précédente, cela présente une plus grande fiabilité.

Lorsque le PC démarre, AnyConnect envoie une authentification de machine uniquement, car aucune information utilisateur n'est disponible. Cependant, lors de la connexion de l’utilisateur, AnyConnect envoie simultanément les informations d’identification de l’ordinateur et de l’utilisateur. En outre, si vous devenez déconnecté ou débranchez/rebranchez le câble, les informations d'identification de l'ordinateur et de l'utilisateur sont à nouveau envoyées dans une authentification EAP-FAST unique, qui diffère des versions précédentes d'AnyConnect sans chaînage EAP.

EAP-TEAP est la meilleure solution à long terme car elle est faite spécialement pour prendre en charge ce type d'authentification, mais EAP-TEAP n'est toujours pas pris en charge dans le demandeur natif de nombreux systèmes d'exploitation à ce jour