Ventajas y ventajas de la restricción del acceso a máquinas

Contenido

Introducción

Este documento describe un problema encontrado con la restricción de acceso a máquina (MAR) y proporciona una solución al problema.

Con el crecimiento de los dispositivos personales, es más importante que nunca que los administradores de sistemas ofrezcan una forma de restringir el acceso a ciertas partes de la red únicamente a los activos corporativos. El problema descrito en este documento se refiere a cómo identificar de forma segura estas áreas de interés y autenticarlas sin interrumpir la conectividad de los usuarios.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de 802.1x para entender completamente este documento. Este documento asume la familiaridad con la autenticación 802.1x del usuario, y resalta los problemas y ventajas ligados al uso de MAR, y más generalmente, a la autenticación de máquina.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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.

Problema

MAR básicamente intenta resolver un problema común inherente a la mayoría de los métodos actuales y populares del protocolo de autenticación extensible (EAP), a saber, que la autenticación de máquina y la autenticación de usuario son procesos independientes y no relacionados.

La autenticación de usuario es un método de autenticación 802.1x que la mayoría de los administradores del sistema conocen. La idea es que las credenciales (nombre de usuario/contraseña) se otorguen a cada usuario y que el conjunto de credenciales representa una persona física (también puede ser compartida entre varias personas). Por lo tanto, un usuario puede iniciar sesión desde cualquier lugar de la red con esas credenciales.

Una autenticación de máquina es técnicamente la misma, pero normalmente al usuario no se le pide que introduzca las credenciales (o el certificado); el ordenador o la máquina lo hace por su cuenta. Esto requiere que la máquina ya tenga las credenciales almacenadas. El nombre de usuario enviado es **host/<MyPCHostname>**, siempre que su máquina tenga **<MyPCHostname>** establecido como nombre de host. En otras palabras, envía **host/** seguido de su nombre de host.

Aunque no está directamente relacionado con Microsoft Windows y Cisco Active Directory, este proceso se representa más fácilmente si la máquina se une a Active Directory porque el nombre de host del equipo se agrega a la base de datos de dominio y las credenciales se negocian (y se renuevan cada 30 días de forma predeterminada) y se almacenan en la máquina. Esto significa que la autenticación de la máquina es posible desde cualquier tipo de dispositivo, pero es mucho más fácil y transparente si la máquina se une a Active Directory y las credenciales permanecen ocultas al usuario.

MAR como solución

Es fácil decir que la solución es que Cisco Access Control System (ACS) o Cisco Identity Services Engine (ISE) completen el MAR, pero hay ventajas y desventajas que tener en cuenta antes de implementarlo. La mejor forma de implementar esto es en las guías de usuario de ACS o ISE, por lo que este documento simplemente describe si se debe considerar o no, y algunos posibles obstáculos.

Las ventajas

MAR se inventó porque las autenticaciones de usuario y máquina son totalmente independientes. Por lo tanto, el servidor RADIUS no puede imponer una verificación donde los usuarios deben iniciar sesión desde los dispositivos propiedad de la empresa. Con MAR, el servidor RADIUS (ACS o ISE, en el lado de Cisco) aplica, para una autenticación de usuario determinada, que debe haber una autenticación de máquina válida en las X horas (normalmente 8 horas, pero esto es configurable) que preceden a la autenticación de usuario para el mismo terminal.

Por lo tanto, una autenticación de máquina se realiza correctamente si el servidor RADIUS conoce las credenciales de la máquina, normalmente si la máquina se une al dominio, y el servidor RADIUS lo verifica con una conexión al dominio. Incumbe enteramente al administrador de la red determinar si una autenticación correcta de la máquina proporciona acceso completo a la red o sólo un acceso restringido; normalmente, al menos se abre la conexión entre el cliente y

Active Directory para que el cliente pueda realizar acciones como la renovación de la contraseña de usuario o la descarga de objetos de directiva de grupo (GPO).

Si una autenticación de usuario proviene de un dispositivo en el que no se ha realizado una autenticación de máquina en las horas anteriores, se deniega al usuario, incluso si el usuario es normalmente válido.

El acceso completo sólo se concede a un usuario si la autenticación es válida y se completa desde un terminal en el que se ha producido una autenticación de máquina en las últimas dos horas.

Los Cons

Esta sección describe los inconvenientes del uso de MAR.

MAR y Microsoft Windows Supplicant

La idea detrás de MAR es que para que una autenticación de usuario tenga éxito, no sólo debe que ese usuario tenga credenciales válidas, sino que también se debe registrar una autenticación de máquina exitosa desde ese cliente. Si hay algún problema con eso, el usuario no puede autenticarse. El problema que surge es que esta función a veces puede bloquear inadvertidamente a un cliente legítimo, lo que obliga al cliente a reiniciarse para recuperar el acceso a la red.

Microsoft Windows sólo realiza la autenticación de la máquina en el momento del inicio (cuando aparece la pantalla de inicio de sesión); tan pronto como el usuario ingresa las credenciales del usuario, se realiza una autenticación de usuario. Además, si el usuario cierra la sesión (vuelve a la pantalla de inicio de sesión), se realiza una nueva autenticación del equipo.

Este es un ejemplo de escenario que muestra por qué el MAR a veces causa problemas:

El usuario X trabajó todo el día en su portátil, que se conectó mediante una conexión inalámbrica. Al final del día, simplemente cierra el portátil y deja el trabajo. Esto coloca al portátil en una situación de hibernación. Al día siguiente, regresa a la oficina y abre su portátil. Ahora, no puede establecer una conexión inalámbrica.

Cuando Microsoft Windows hiberna, toma una instantánea del sistema en su estado actual, que incluye el contexto de quién ha iniciado sesión. De la noche a la mañana, la entrada en caché de MAR para el portátil del usuario caduca y se depura. Sin embargo, cuando el portátil está encendido, no realiza una autenticación del equipo. En su lugar, se dirige directamente a una autenticación de usuario, ya que eso fue lo que registró la hibernación. La única manera de resolver esto es cerrar la sesión del usuario o reiniciar su equipo.

Aunque el MAR es una buena función, puede causar interrupciones en la red. Estas interrupciones son difíciles de resolver hasta que entienda cómo funciona MAR; cuando implementa MAR, es importante educar a los usuarios finales sobre cómo apagar correctamente los ordenadores y cerrar la sesión de cada máquina al final de cada día.

MAR y varios servidores RADIUS

Es común tener varios servidores RADIUS en la red con fines de balanceo de carga y

redundancia. Sin embargo, no todos los servidores RADIUS soportan una memoria caché de sesión MAR compartida. Solamente las versiones 5.4 y posteriores de ACS, y la versión 2.3 de ISE y posteriores soportan la sincronización de caché MAR entre nodos. Antes de estas versiones, no es posible realizar una autenticación de máquina contra un servidor ACS/ISE, y realizar una autenticación de usuario contra otro, ya que no se corresponden entre sí.

Switching de red por cable e inalámbrica

La memoria caché MAR de muchos servidores RADIUS depende de la dirección MAC. Se trata simplemente de una tabla con la dirección MAC de los portátiles y la marca de tiempo de su última autenticación de máquina exitosa. De esta manera, el servidor puede saber si el cliente fue autenticado en las últimas X horas.

Sin embargo, ¿qué sucede si arranca el portátil con una conexión por cable (y, por lo tanto, realiza una autenticación de la máquina desde su MAC con cables) y luego cambia a una red inalámbrica durante el día? El servidor RADIUS no tiene forma de relacionar su dirección MAC inalámbrica con su dirección MAC con cables y de saber que fue autenticado en las últimas X horas. La única forma es cerrar la sesión y hacer que Microsoft Windows realice otra autenticación de equipo a través de la red inalámbrica.

Solución

Entre otras muchas funciones, Cisco AnyConnect cuenta con la ventaja de perfiles preconfigurados que activan la autenticación de usuarios y equipos. Sin embargo, se encuentran las mismas limitaciones que se ven con el suplicante de Microsoft Windows, con respecto a que la autenticación del equipo sólo se produce cuando se desconecta o se reinicia.

Además, con las versiones 3.1 y posteriores de AnyConnect, es posible realizar EAP-FAST con encadenamiento de EAP. Se trata básicamente de una autenticación única, donde se envían dos pares de credenciales, el nombre de usuario/contraseña de la máquina y el nombre de usuario/contraseña del usuario, al mismo tiempo. ISE, por lo tanto, comprueba con mayor facilidad que ambas son exitosas. Sin memoria caché usada y sin necesidad de recuperar una sesión anterior, esto presenta una mayor confiabilidad.

Cuando se inicia el PC, AnyConnect sólo envía una autenticación del equipo, ya que no hay información de usuario disponible. Sin embargo, al iniciar sesión el usuario, AnyConnect envía las credenciales del equipo y del usuario simultáneamente. Además, si se desconecta o desconecta/reconecta el cable, tanto la máquina como las credenciales de usuario se envían de nuevo en una única autenticación EAP-FAST, que difiere de las versiones anteriores de AnyConnect sin encadenamiento de EAP.

EAP-TEAP es la mejor solución a largo plazo, ya que se realiza especialmente para admitir este tipo de autenticaciones, pero EAP-TEAP todavía no se soporta en el suplicante nativo de muchos sistemas operativos hasta el día de hoy