Prós e contras da restrição de acesso à máquina

Contents

Introduction

Este documento descreve um problema encontrado com a Restrição de Acesso à Máquina (MAR - Machine Access Restriction) e fornece uma solução para o problema.

Com o crescimento de dispositivos pessoais, é mais importante que os administradores de sistema sempre forneçam uma maneira de restringir o acesso a certas partes da rede apenas a ativos corporativos. O problema descrito neste documento diz respeito a como identificar com segurança essas áreas de preocupação e autenticá-las sem interrupções na conectividade do usuário.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do 802.1x para entender totalmente este documento. Este documento assume familiaridade com a autenticação 802.1x do usuário e destaca os problemas e as vantagens associados ao uso do MAR e, de modo mais geral, a autenticação da máquina.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

O MAR basicamente tenta resolver um problema comum inerente na maioria dos métodos atuais e populares de Protocolo de Autenticação Extensível (EAP - Extensible Authentication Protocol), a saber, que a autenticação da máquina e a autenticação do usuário são processos separados e não relacionados.

A autenticação de usuário é um método de autenticação 802.1x familiar à maioria dos administradores do sistema. A ideia é que as credenciais (nome de usuário/senha) sejam dadas a cada usuário e que esse conjunto de credenciais represente uma pessoa física (também pode ser compartilhado entre várias pessoas). Portanto, um usuário pode fazer login de qualquer lugar na rede com essas credenciais.

A autenticação de uma máquina é tecnicamente a mesma, mas o usuário não é normalmente solicitado a inserir as credenciais (ou certificado); o computador ou a máquina faz isso sozinho. Isso exige que a máquina já tenha credenciais armazenadas. O nome de usuário enviado é **host/<MyPCHostname>**, desde que sua máquina tenha **<MyPCHostname>** definido como um nome de host. Em outras palavras, ele envia **host/** seguido do seu nome de host.

Embora não esteja diretamente relacionado ao Microsoft Windows e ao Cisco Ative Diretory, esse processo é renderizado mais facilmente se a máquina estiver associada ao Ative Diretory porque o nome de host do computador é adicionado ao banco de dados de domínio, e as credenciais são negociadas (e renovadas a cada 30 dias por padrão) e armazenadas na máquina. Isso significa que a autenticação da máquina é possível de qualquer tipo de dispositivo, mas ela é renderizada de forma muito mais fácil e transparente se a máquina estiver conectada ao Ative Diretory e as credenciais permanecerem ocultas do usuário.

MAR como solução

Éfácil dizer que a solução é que o Cisco Access Control System (ACS) ou o Cisco Identity Services Engine (ISE) concluam o MAR, mas há vantagens e desvantagens a serem consideradas antes que isso seja implementado. Como implementar isso é melhor descrito nos guias de usuário do ACS ou do ISE, portanto, este documento simplesmente descreve se deve ou não considerá-lo e alguns possíveis bloqueios.

Os Prós

O MAR foi inventado porque as autenticações de usuário e máquina são totalmente separadas. Portanto, o servidor RADIUS não pode impor uma verificação na qual os usuários devem fazer login a partir de dispositivos de propriedade da empresa. Com o MAR, o servidor RADIUS (ACS ou ISE, no lado da Cisco) reforça, para uma dada autenticação de usuário, que deve haver uma autenticação de máquina válida nas X horas (normalmente 8 horas, mas isso é configurável) que precede a autenticação de usuário para o mesmo endpoint.

Portanto, a autenticação de uma máquina será bem-sucedida se as credenciais da máquina forem conhecidas pelo servidor RADIUS, geralmente se a máquina estiver associada ao domínio, e o servidor RADIUS verificará isso com uma conexão ao domínio. Cabe inteiramente ao administrador da rede determinar se uma autenticação de máquina bem-sucedida fornece acesso total à rede ou apenas um acesso restrito; normalmente, isso abre pelo menos a conexão entre o cliente e o Ative Diretory para que o cliente possa executar ações como renovação da senha do usuário ou fazer download de Objetos de Política de Grupo (GPOs).

Se uma autenticação de usuário for proveniente de um dispositivo em que não ocorreu uma autenticação de máquina nas duas horas anteriores, o usuário será negado, mesmo que o

usuário seja normalmente válido.

O acesso total só é concedido a um usuário se a autenticação for válida e concluída de um endpoint onde ocorreu uma autenticação de máquina nas últimas horas.

Os Cons

Esta seção descreve os contras do uso de MAR.

Requerente do MAR e Microsoft Windows

A ideia por trás do MAR é que, para que uma autenticação de usuário seja bem-sucedida, esse usuário não só deve ter credenciais válidas, como também deve ser registrada uma autenticação de máquina bem-sucedida desse cliente. Se houver algum problema com isso, o usuário não poderá autenticar. O problema que surge é que esse recurso às vezes pode inadvertidamente bloquear um cliente legítimo, o que força o cliente a reinicializar para recuperar o acesso à rede.

O Microsoft Windows executa a autenticação da máquina somente no momento da inicialização (quando a tela de login é exibida); assim que o usuário entra nas credenciais do usuário, uma autenticação de usuário é executada. Além disso, se o usuário fizer logoff (retorna à tela de login), uma nova autenticação de máquina será executada.

Este é um exemplo de cenário que mostra por que o MAR às vezes causa problemas:

O usuário X trabalhou o dia inteiro em seu laptop, que estava conectado por uma conexão sem fio. No fim das contas, ele simplesmente fecha o laptop e deixa o trabalho. Isso coloca o laptop em hibernação. No dia seguinte, ele volta para o escritório e abre seu laptop. Agora, ele não consegue estabelecer uma conexão sem fio.

Quando o Microsoft Windows hibernar, ele faz um snapshot do sistema em seu estado atual, o que inclui o contexto de quem fez logon. Durante a noite, a entrada do MAR armazenada em cache para o laptop do usuário expira e é removida. No entanto, quando o notebook está ligado, ele não executa uma autenticação de máquina. Em vez disso, vai diretamente para a autenticação de um usuário, já que isso foi o que a hibernação registrou. A única maneira de resolver isso é desconectar o usuário ou reinicializar o computador.

Embora o MAR seja um bom recurso, ele tem o potencial de causar interrupções na rede. Essas interrupções são difíceis de solucionar até que você entenda como o MAR funciona; ao implementar o MAR, é importante informar os usuários finais sobre como desligar corretamente os computadores e desconectar de cada máquina no final de cada dia.

MAR e vários servidores RADIUS

Écomum ter vários servidores RADIUS na rede para fins de balanceamento de carga e redundância. No entanto, nem todos os servidores RADIUS suportam um cache de sessão MAR compartilhado. Somente as versões 5.4 e posterior do ACS e a versão 2.3 e posterior do ISE suportam a sincronização de cache MAR entre nós. Antes dessas versões, não é possível executar uma autenticação de máquina em um servidor ACS/ISE e executar uma autenticação de usuário em relação a outro, pois eles não correspondem entre si.

MAR e switching com e sem fio

O cache MAR de muitos servidores RADIUS depende do endereço MAC. É simplesmente uma tabela com o endereço MAC dos notebooks e o carimbo de data e hora da última autenticação bem-sucedida da máquina. Dessa forma, o servidor pode saber se o cliente foi autenticado pela máquina nas últimas X horas.

No entanto, o que acontece se você inicializa seu notebook com uma conexão com fio (e, portanto, faz uma autenticação de máquina a partir do seu MAC com fio) e depois muda para o wireless durante o dia? O servidor RADIUS não tem como correlacionar seu endereço MAC sem fio com seu endereço MAC com fio e saber que você foi autenticado pela máquina nas últimas X horas. A única maneira é fazer logoff e fazer com que o Microsoft Windows conduza outra autenticação de máquina via rede sem fio.

Solução

Entre muitos outros recursos, o Cisco AnyConnect tem a vantagem de perfis pré-configurados que acionam a autenticação de máquina e usuário. No entanto, são encontradas as mesmas limitações do suplicante do Microsoft Windows, com relação à autenticação da máquina que só ocorre quando você faz logoff ou reinicializa.

Além disso, com as versões 3.1 e posteriores do AnyConnect, é possível executar EAP-FAST com encadeamento EAP. Basicamente, trata-se de uma única autenticação, na qual você envia dois pares de credenciais, o nome de usuário/senha da máquina e o nome de usuário/senha do usuário, ao mesmo tempo. O ISE, então, verifica mais facilmente se ambos foram bem-sucedidos. Sem cache usado e sem necessidade de recuperar uma sessão anterior, isso apresenta maior confiabilidade.

Quando o PC é inicializado, o AnyConnect envia apenas uma autenticação de máquina, porque nenhuma informação de usuário está disponível. No entanto, após o login do usuário, o AnyConnect envia as credenciais da máquina e do usuário simultaneamente. Além disso, se você for desconectado ou desconectar/reconectar o cabo, as credenciais da máquina e do usuário serão enviadas novamente em uma única autenticação EAP-FAST, que difere das versões anteriores do AnyConnect sem encadeamento de EAP.

EAP-TEAP é a melhor solução a longo prazo, pois é feita especialmente para suportar esses tipos de autenticação, mas o EAP-TEAP ainda não é suportado no suplicante nativo de muitos SO desde hoje