Profissionais da restrição de acesso da máquina - e - contra

Índice

Introdução

Este documento descreve um problema encontrado com restrição de acesso da máquina (MARÇO), e fornece uma solução ao problema.

Com o crescimento de dispositivos pessoalmente-possuídos, é mais importante que nunca para administradores de sistema fornecer uma maneira de restringir o acesso a determinadas partes da rede aos ativos corporativo-possuídos somente. O problema descrito em interesses deste documento como identificar firmemente estas áreas de preocupação e autenticá-las sem rompimentos à conectividade de usuário.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do 802.1x a fim compreender inteiramente este documento. Este documento supõe a familiaridade com a autenticação do 802.1x do usuário, e destaca os problemas e as vantagens amarrado ao uso de MARÇO, e mais geralmente, autenticação da máquina.

Componentes Utilizados

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto

potencial de qualquer comando.

Problema

MARÇO tenta basicamente resolver um problema comum inerente na maioria dos métodos atuais e populares do Extensible Authentication Protocol (EAP), a saber essas autenticação e autenticação de usuário da máquina são processos separados, não relacionados.

A autenticação de usuário é um método de autenticação do 802.1x que seja familiar à maioria de administradores de sistema. A ideia é que as credenciais (username/senha) estão dadas a cada usuário, e que o grupo de credenciais representa uma pessoa física (pode ser compartilhado entre diversos povos também). Consequentemente, um usuário pode entrar em qualquer lugar dentro da rede com aquelas credenciais.

Uma autenticação da máquina é tecnicamente a mesma, mas o usuário não é alertado tipicamente entrar nas credenciais (ou no certificado); o computador ou a máquina fazem aquele no seus próprios. Isto exige a máquina já ter as credenciais armazenadas. O username enviado é **host/<MyPCHostname>**, contanto que sua máquina tem o <MyPCHostname > ajustado como um hostname. Ou seja envia o **anfitrião** seguido por seu hostname.

Embora relativo não diretamente a Microsoft Windows e ao diretório ativo de Cisco, este processo está rendido mais facilmente se a máquina é juntada ao diretório ativo porque o hostname do computador está adicionado ao base de dados de domínio, e as credenciais são negociadas (e renovou cada 30 dias à revelia) e armazenadas na máquina. Isto significa que a autenticação da máquina é possível de qualquer tipo de dispositivo, mas está rendida muito mais facilmente e transparentemente se a máquina é juntada ao diretório ativo, e as credenciais ficam hidden do usuário.

MARÇO como uma solução

Éfácil dizer que a solução é para o sistema de controle de acesso (ACS) de Cisco ou o Cisco Identity Services Engine (ISE) para terminar MARÇO, mas há umas vantagens e uns inconvenientes a considerar antes que este esteja executado. Como executar isto é descrita melhor em Guias do Usuário ACS ou ISE, assim que este documento descreve simplesmente mesmo se considerar o, e alguns cortes de estrada possíveis.

Os profissionais

MARÇO foi inventado porque as autenticações do usuário e da máquina são totalmente separadas. Consequentemente, o servidor Radius não pode reforçar uma verificação onde os usuários devam entrar dos dispositivos da empresa. Com MARÇO, o servidor Radius (ACS ou ISE, no Cisco-lado) reforça, para uma autenticação de usuário dada, que deve haver uma autenticação válida da máquina nas horas X (tipicamente 8 horas, mas nesta é configurável) que precede a autenticação de usuário para o mesmo valor-limite.

Consequentemente, uma autenticação da máquina sucede se as credenciais da máquina são sabidas pelo servidor Radius, tipicamente se a máquina é juntada ao domínio, e o servidor Radius verifica este com uma conexão ao domínio. É inteiramente até o administrador de rede para determinar se uma autenticação bem sucedida da máquina fornece o acesso direto à rede, ou somente um acesso restrito; tipicamente, isto abre pelo menos a conexão entre o cliente e o diretório ativo de modo que o cliente possa executar ações como a renovação dos objetos da

política do grupo da senha do usuário ou da transferência (GPOs).

Se uma autenticação de usuário vem de um dispositivo onde uma autenticação da máquina não ocorra nos pares precedentes de horas, a seguir o usuário é negado, mesmo se o usuário é normalmente válido.

O acesso direto está concedido somente a um usuário se a autenticação é válida e terminada de um valor-limite onde uma autenticação da máquina ocorra nos pares passados de horas.

O contra

Esta seção descreve o contra do uso de MARÇO.

MARÇO e suplicante de Microsoft Windows

A ideia atrás de MARÇO é aquela para que uma autenticação de usuário suceda, deve não somente que o usuário tem credenciais válidas, mas uma autenticação bem sucedida da máquina deve ser registrada desse cliente também. Se há qualquer problema com esse, o usuário não pode autenticar. A edição que elevara é que esta característica pode às vezes inadvertidamente fechamento um cliente legítimo, que force o cliente a recarregar a fim recuperar o acesso à rede.

Microsoft Windows executa a autenticação da máquina somente no tempo de inicialização (quando a tela de login aparece); assim que o usuário incorporar as credenciais do usuário, uma autenticação de usuário está executada. Também, se o usuário termina (retornos à tela de login), uma autenticação nova da máquina é executada.

Está aqui um exemplo de cenário que mostre porque MARÇO causa às vezes problemas:

O usuário X trabalhou o dia inteiro em seu portátil, que foi conectado através de uma conexão Wireless. No final do dia, fecha simplesmente o portátil e as folhas funcionam. Isto coloca o portátil na hibernação. O next day, volta no escritório e abre seu portátil. Agora, é incapaz de estabelecer uma conexão Wireless.

Quando Microsoft Windows hiberna, toma um instantâneo do sistema em seu estado atual, que inclui o contexto de quem foi entrado. Durante a noite, a entrada março-posta em esconderijo para o portátil do usuário expira e é removida. Contudo, quando o portátil é posto sobre, não executa uma autenticação da máquina. Entra pelo contrário em linha reta em uma autenticação de usuário, desde que aquele era o que a hibernação gravou. A única maneira de resolver isto é registrar fora o usuário, ou recarregar seu computador.

Embora MARÇO seja uma boa característica, tem o potencial causar o rompimento de rede. Estes rompimentos são difíceis de pesquisar defeitos até que você compreenda que a maneira MARÇO trabalha; quando você executa MARÇO, é importante educar os utilizadores finais sobre como fechar corretamente computadores e terminar de cada máquina no fim de cada dia.

MARÇO e vários servidores Radius

Écomum ter diversos servidores Radius na rede para a função de balanceamento de carga e os fins de redundância. Contudo, não todos os servidores Radius apoiam um esconderijo compartilhado da sessão de MARÇO. Somente versões de ACS 5.4 e mais atrasado, e sincronização do esconderijo de MARÇO do apoio da versão 2.2 e mais recente ISE entre Nós.

Antes destas versões, não é possível executar uma autenticação da máquina contra um server ACS/ISE, e executar uma autenticação de usuário contra outro, porque não correspondem um com o otro.

MARÇO e interruptor do Prender-Sem fio

O esconderijo de MARÇO de muitos servidores Radius confia no MAC address. É simplesmente uma tabela com o MAC address dos portáteis e do timestamp de sua última autenticação bem sucedida da máquina. Esta maneira, o server pode saber se o cliente era máquina autenticada nas últimas horas X.

Contudo, que acontece se você carreg seu portátil com uma conexão ligada com fio (e faz consequentemente uma autenticação da máquina de seu MAC prendido) e o comuta então ao Sem fio durante o dia? O servidor Radius não tem nenhum meio correlacionar seu MAC address wireless com seu MAC address prendido e saber que você era máquina autenticada nas horas passadas X. A única maneira é terminar e mandar Microsoft Windows conduzir uma outra autenticação da máquina através do Sem fio.

Solução

Entre muitos outros recursos, Cisco AnyConnect tem a vantagem dos perfis PRE-configurados que provocam a máquina e a autenticação de usuário. Contudo, as mesmas limitações que consideradas com suplicante de Microsoft Windows estão encontradas, a propósito da autenticação da máquina que ocorre somente quando você termina ou recarrega.

Também, com versões 3.1 e mais recente de AnyConnect, é possível executar EAP-FAST com o EAP-encadeamento. Esta é basicamente uma única autenticação, onde você envie dois pares de credenciais, do username da máquina/senha e o username do usuário/senha, ao mesmo tempo. O ISE, então, certifica-se de mais facilmente ambos sejam bem sucedidos. Sem o esconderijo usado e a nenhuma necessidade recuperar uma sessão precedente, isto apresenta a maior confiança.

Quando as botas PC, AnyConnect enviarem uma autenticação da máquina somente, porque nenhuma informação sobre o usuário está disponível. Contudo, em cima do login de usuário, AnyConnect envia os credentails da máquina e do usuário simultaneamente. Também, se você se torna desligado ou se desconecta/replug o cabo, a máquina e usuário que as credenciais são enviadas outra vez em uma única autenticação EAP-FAST, que difira das versões anterior de AnyConnect sem EAP-acorrentar.

EAP-TEAP é a melhor solução a longo prazo porque é feito especialmente para apoiar estes tipo de autenticações, mas EAP-TEAP não é apoiado ainda no suplicante nativo de muito OS até à data deste dia