Machine Access Restriction Pros and Cons

Contents

Introduction

This document describes a problem encountered with Machine Access Restriction (MAR), and provides a solution to the problem.

With the growth of personally-owned devices, it is more important that ever for system administrators to provide a way to restrict access to certain parts of the network to corporately-owned assets only. The problem described in this document concerns how to securely identify these areas of concern and authenticate them without disruptions to user connectivity.

Prerequisites

Requirements

Cisco recommends that you have knowledge of 802.1x in order to fully understand this document. This document assumes familiarity with user 802.1x authentication, and highlights the problems and advantages tied to the use of MAR, and more generally, machine authentication.

Components Used

This document is not restricted to specific software and hardware versions.

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.

Problem

MAR basically attempts to solve a common problem inherent in most of the current and popular Extensible Authentication Protocol (EAP) methods, namely that machine authentication and user authentication are separate, unrelated processes.

User authentication is a 802.1x authentication method that is familiar to most system administrators. The idea is that credentials (username/password) are given to each user, and that set of credentials represents a physical person (it can be shared between several people as well). Therefore, a user can log in from anywhere in the network with those credentials.

A machine authentication is technically the same, but the user is typically not prompted to enter the credentials (or certificate); the computer or machine does that on its own. This requires the machine to already have credentials stored. The username sent is **host/<MyPCHostname**>, provided that your machine has <**MyPCHostname**> set as a hostname. In other words, it sends **host/** followed by your hostname.

Although not directly related to Microsoft Windows and Cisco Active Directory, this process is rendered more easily if the machine is joined to Active Directory because the computer hostname is added to the domain database, and credentials are negotiated (and renewed every 30 days by default) and stored on the machine. This means that machine authentication is possible from any type of device, but it is rendered much more easily and transparently if the machine is joined to Active Directory, and credentials stay hidden from the user.

MAR as a Solution

It is easy to say that the solution is for Cisco Access Control System (ACS) or Cisco Identity Services Engine (ISE) to complete MAR, but there are advantages and drawbacks to consider before this is implemented. How to implement this is best described in ACS or ISE user-guides, so this document simply describes whether or not to consider it, and some possible roadblocks.

The Pros

MAR was invented because user and machine authentications are totally separate. Therefore, the RADIUS server cannot enforce a verification where users must log in from company-owned devices. With MAR, the RADIUS server (ACS or ISE, on the Cisco-side) enforces, for a given user authentication, that there must be a valid machine authentication in the X hours (typically 8 hours, but this is configurable) that precedes the user authentication for the same endpoint.

Therefore, a machine authentication succeeds if the machine credentials are known by the RADIUS server, typically if the machine is joined to the domain, and the RADIUS server verifies this with a connection to the domain. It is entirely up to the network administrator to determine if a successful machine authentication provides full access to the network, or only a restricted access; typically, this at least opens the connection between the client and the Active Directory so that the client can perform such actions as renewal of the user password or download Group Policy Objects (GPOs).

If a user authentication comes from a device where a machine authentication has not occured in the previous couple of hours, then the user is denied, even if the user is normally valid.

Full access is only granted to a user if authentication is valid and completed from an endpoint where a machine authentication occured in the past couple of hours.

The Cons

This section describes the cons of MAR use.

MAR and Microsoft Windows Supplicant

The idea behind MAR is that for a user authentication to suceed, not only must that user have valid credentials, but a successful machine authentication must be logged from that client as well. If there is any problem with that, the user cannot authenticate. The issue that arises is that this feature can sometimes inadvertently lock-out a legitimate client, which forces the client to reboot in order to regain access to the network.

Microsoft Windows performs machine authentication only at boot-time (when the login screen appears); as soon as the user enters the user credentials, a user authentication is performed. Also, if the user logs off (returns to the login screen), a new machine authentication is performed.

Here is an example scenario that shows why MAR sometimes causes problems:

User X worked all day on his laptop, which was connected via a wireless connection. At the end of the day, he simply closes the laptop and leaves work. This places the laptop into hibernation. The next day, he comes back into the office and opens his laptop. Now, he is unable to establish a wireless connection.

When Microsoft Windows hibernates, it takes a snapshot of the system in its current state, which includes the context of who was logged in. Overnight, the MAR-cached entry for the user laptop expires and is purged. However, when the laptop is powered on, it does not perform a machine authentication. It instead goes straight into a user authentication, since that was what the hibernation recorded. The only way to resolve this is to log the user off, or to reboot his computer.

Although MAR is a good feature, it has the potential to cause network disruption. These disruptions are difficult to troubleshoot until you understand the way MAR works; when you implement MAR, it is important to educate the end-users about how to properly shut down computers and log off from every machine at the end of each day.

MAR and Various RADIUS Servers

It is common to have several RADIUS servers in the network for load-balancing and redundancy purposes. However, not all RADIUS servers support a shared MAR session cache. Only ACS Versions 5.4 and later, and ISE version 2.3 and later support MAR cache synchronization between nodes. Before these versions, it is not possible to perform a machine authentication against one ACS/ISE server, and to perform a user authentication against another, as they do not correspond with each other.

MAR and Wired-wireless Switching

The MAR cache of many RADIUS servers relies on the MAC address. It is simply a table with the MAC address of laptops and the timestamp of their last successful machine authentication. This way, the server can know if the client was machine authenticated in the last X hours.

However, what happens if you boot your laptop with a wired connection (and therefore do a machine authentication from your wired MAC) and then switch to wireless during the day? The RADIUS server has no means to correlate your wireless MAC address with your wired MAC address and to know that you were machine authenticated in the past X hours. The only way is to

log off and have Microsoft Windows conduct another machine authentication via wireless.

Solution

Among many other features, Cisco AnyConnect has the advantage of pre-configured profiles that trigger machine and user authentication. However, the same limitations as seen with Microsoft Windows supplicant are encountered, with regards to machine authentication only occuring when you log off or reboot.

Also, with AnyConnect Versions 3.1 and later, it is possible to perform EAP-FAST with EAP-chaining. This is basically a single authentication, where you send two pairs of credentials, the machine username/password and the user username/password, at the same time. ISE, then, more easily checks that both are successfull. With no cache used and no need to retrieve a previous session, this presents greater reliability.

When the PC boots, AnyConnect sends a machine authentication only, because no user information is available. However, upon user login, AnyConnect sends both the machine and user credentails simultaneously. Also, if you become disconnected or unplug/replug the cable, both the machine and user credentials are again sent in a single EAP-FAST authentication, which differs from the earlier versions of AnyConnect without EAP-chaining.

EAP-TEAP is the long term best solution as it is made especially to support these type of authentications, but EAP-TEAP is still not supported in the native supplicant of many OS as of this day