Milton
SECURITY GROUP

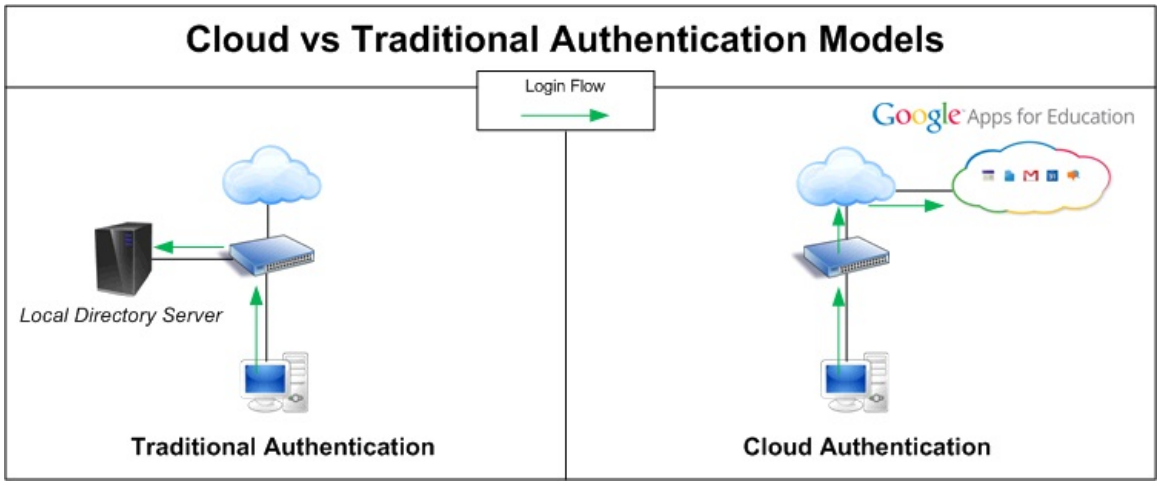
Local Network Security Using Google Apps for Education

Milton
SECURITY GROUP

Table of contents

Network Authentication Overview

Network authentication has always been a prevalent topic in the Networking field. As it implies, authentication is the process by which the network determines whether or not the person logging in is the “authentic” you. As society continues to integrate more and more technology in to our daily lives (i.e. The Internet of Things), authentication systems will need to adapt to support ever-changing security challenges. With so many different kinds of mobile phones, tablets, and the recent introduction of "The Cloud", authentication becomes increasingly vital. Milton Security Group’s Adaptive Security solutions provide IT professionals with unprecedented management possibilities by allowing them to know exactly who is on their network, what device they are using, and where they are connecting. The solution provides security above and beyond simple authentication.



Milton
SECURITY GROUP

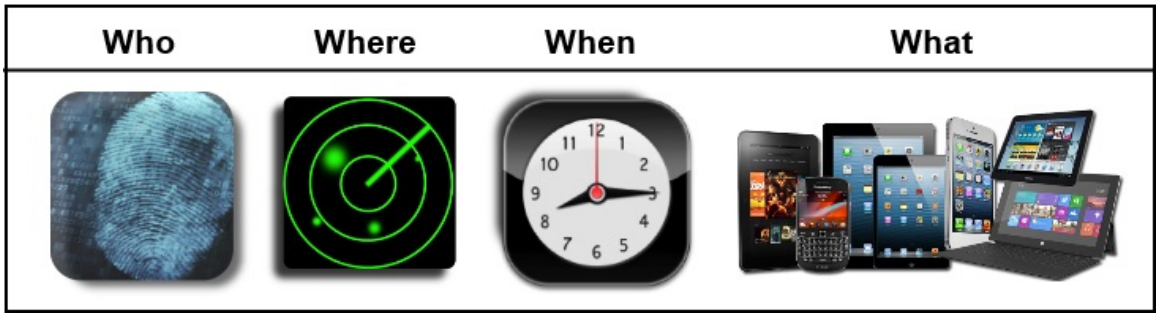
Network Security Overview

To access resources on a network, users require a set of credentials. Needing to remember yet another username and password can be seem like an extra burden, causing some people to reuse the same set they use for multiple other sites like social media, banking and gaming. The reuse of passwords is one of the most common mistakes people make as it compromises many networks at once when a password is leaked. Another common mistake that people make, when they're feeling lazy about security, is to use an extremely simple username and password on both encrypted and unencrypted sites. This can also put your network in jeopardy.

So, what can be done to help alleviate this stress from your students and faculty when you are not using an enterprise level authentication method like Active Directory? Utilize an existing form of authentication via cloud services, such as Google Apps for Education. The user's school email login gains them secure access to their Google Apps for Education account, without the stress of yet another username and password to remember. While there are benefits to using a cloud authentication service(like cloud storage), there are also some difficult challenges that this solution presents. For instance, how do you tie an external login for Google to your internal identification? Knowing exactly who is on your network becomes more difficult when the authentication is hosted in the cloud. What is needed is a

link, something to tie the Google Apps for Education with the internal identity of each device and user.

Before diving into exactly how we establish such a link, lets take a look at what we need to know about the identities of our network users. First, we want to have full and unrestricted visibility of every device connected on our network. The next step is to know exactly what types of devices we're dealing with. Are they district owned machines or personal mobile devices? We also want to know where that user is coming from, what time of day they are connecting, and whether or not the device is healthy. Once we have created this device profile, we need to know exactly who is behind that device which is where the login comes into the process. The compiled list of results produces a profile that fully defines the student or faculty member.



Milton
SECURITY GROUP

Using Google Apps For Education For Authentication

Now that we have our user and device information, we can link it and Google Authentication in order to enforce access in multiple ways. Using different combinations of the information we've obtained, we can control almost any scenario. Using the time of day the person is connecting, and who that person is, allows us to create a simple time-sensitive availability of resources.

Example: *A school has a guest user trying to login at 3am. This user could be locked out using designated hours. However, an Assistant Principal might be allowed on the network at any hour.*

Some situations would only require a single piece of information to enforce security. For instance, we might not allow access to grades from the cafeteria.

Example: *A school wants to stop users from accessing grades via the open Wi-Fi provided for guests in the cafeteria. We can use the location of the traffic origin (the "where") to enforce this security policy. The "where" being Guest Wifi vs. classroom computer.*

The level of criteria can be complex and use many factors to get very granular:

Example: *Students need to access a test-taking server, but you want to limit the how and when:*

**You only want them to have access from 2-3pm*

**They must use school-provided devices that have only the test taking software installed*

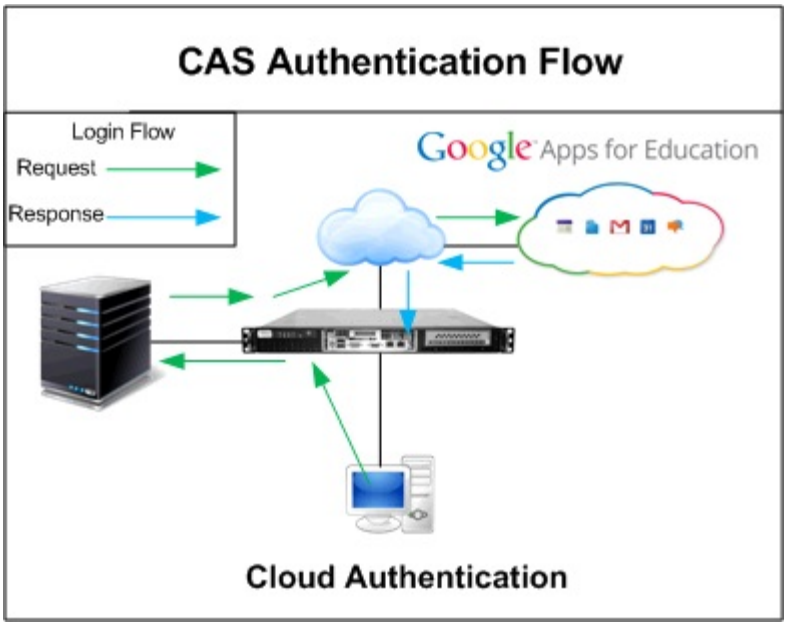
**You want to block access to all other resources, including the internet*

No problem! We would create a policy that allows only devices with certain MAC address to gain access to the testing server. Upon login, the device would be scanned to verify that only the required software is installed.

The adaptive scenarios that are possible from this data reduce your risk, and allow for a granular view of, and control over, what is happening on your network.

Tying Cloud and Local Authentication With Inline Security

The CAS integration with Google Apps for Education uses the OAuth 2.0 protocol, which is currently what Google recommends to be used with all of their services. However, while OAuth 2.0 is prefered, CAS also provides support for deprecated OAuth 1.0 for those who have not migrated to the new version. When users login with the Google Apps for Education Authenticator, the Edge7200i security appliance accepts that login immediately because its been approved by Google. The Edge7200i then queries for the user's organizational unit, which is used in assigning the rights allowed on the school network. This minimizes the impact on your network as users log in and out.



So what exactly is required for this level of control over your authentication? The Milton Security Group CAS solution works in tandem with the Milton Security Group Inline security appliances to provide a seamless environment with Google Apps for Education Authentication servers. When combined with other features offered on the Milton Security Edge and ICEGuard solutions(bandwidth throttling, user access levels, OS compliance (patch, updates, version type) etc.), the overall access level of every person that is connected to your network is highly controlled.

