SecureAuth Cisco ASA VPN Integration End-User Experience: SSL VPN vs. IPSec

Introduction

SecureAuth IdP has the ability to support VPN integrations with all aspects of the Cisco ASA VPN features. Choosing which one is the best fit may depend on the end-user experience that the different access models provide. Cisco features include the Clientless SSL VPN, the SSL VPN Client (AnyConnect), and the IPSec client.

The integration of SecureAuth IdP with the Cisco VPNs is based on the Cisco features that support certificate plus AAA authentication.

SecureAuth IdP enrollment appears essentially the same to the end-user in either case. SecureAuth IdP is a browser-based security service, where the end-user proceeds through a 2-factor authentication process, and then is granted an x.509v3 identity certificate that is used as a second factor, along with the existing enterprise password, to gain access to the protected network or resources.

Since the SecureAuth IdP enrollment process is browser-based, it is an ideal integration with the Clientless SSL VPN. The entire process occurs within a single web-browser session, and the end-user is automatically directed to the enrollment process when a valid certificate is not present. A valid certificate may not exist if the end-user is accessing from a system that has never been used with the VPN, or if the end-user enrolled and the administrator configured lifetime that is granted when certificates are created (i.e. 30, 60, 90 days; 2 weeks, 2 years, 2 minutes).

The enrollment process begins with the end-user opening a browser and landing on the ASA login page, in the case of the Clientless SSL VPN, or pointing directly at the SecureAuth site, when using the IPSec client. This is among the biggest differences in the user experience. The IPSec client is not web-based but SecureAuth IdP is, and so the enrollment process with IPSec will occur “out-of-band” from the actual remote-access process.

After opening a browser the end-user proceeds through a step-wise 2-factor process to assure their identity. After SecureAuth IdP has authenticated the user, a certificate is created and installed on the end-user system which is used during authentication to the VPN.

Re-enrolling is another process that is distinctly different with the different access methods that are available on the Cisco ASA.

The Clientless SSL VPN provides the most seamless experience for the end user. The end-user always uses the URL of the Cisco ASA SSL VPN. Based on whether a certificate is present or not, the ASA directs the end user to Enrollment or Access, which are profile/policy sets configured on the ASA. Once enrolled, the end-user uses the same URL for Access, and the ASA directs them to access where, from the web-browser, the end-user can launch AnyConnect, access sites that are bookmarked, use Smart Tunnels or receive the benefit of other Cisco SSL VPN features.

The AnyConnect client cannot directly enroll with SecureAuth IdP, but behaves in a very similar way. AnyConnect is automatically directed to Enrollment or Access based on the presence of a valid certificate. AnyConnect, when in Enrollment, can automatically invoke the default browser and direct the browser to SecureAuth IdP for enrollment. Or, using Cisco features, a user authenticating in AnyConnect without a certificate can be informed that they need to open a browser to enroll.

The IPSec client offers excellent security, and is often preferred when it is already widely deployed. The IPSec client offers the least flexibility, as it is not capable of leveraging any of the features Cisco has built around the SSL VPN. The IPSec client can use a certificate in the authentication process, but cannot automatically direct the user to the enrollment process. SecureAuth IdP has built-in features to ease the use of the IPSec client. Typically the IPSec client would already have a Connection Profile associated with the VPN, and with a pre-shared key configured. During the enrollment process SecureAuth IdP is able to automatically update existing Connection Profiles, or create new ones, that are bound to the certificate authentication. This means that instead of the end-user needing to make manual changes to the client after enrolling, all they have to do is use the IPSec client in the same manner as they always have (i.e. click on the connect button).

SecureAuth IdP Enrollment

Below is an example of the SecureAuth IdP enrollment process through the Clientless SSL VPN.
In the example above the browser has been opened to the SSL VPN without a valid certificate, and has been directed by the ASA to the Enrollment site. Using a feature in the Cisco SSL VPN the end-user is directed automatically to SecureAuth, where they proceed through the second-factor to authenticate their identity, and a certificate is created on their system.

Clientless SSL VPN Access

After enrolling, if the browser is opened to the SSL VPN, the ASA will request a client certificate.

When a valid certificate is sent to the ASA the ASA will map the session to a connection profile defined by the administrator, such as one set up for access, and the ASA will pre-fill the username from the certificate. The end-user is prompted for their password, and if successful is granted access to the Clientless SSL VPN.

The ASA can be configured to present a portal that is configured with bookmarks or other resources, it can present a custom web-site that is protected by the SSL VPN, or the ASA can automatically launch the AnyConnect client so that the end-user will be connected to the network. Launching AnyConnect automatically essentially creates an environment that can replace the IPSec client, from the user’s perspective, with a web-browser.
AnyConnect Access

Once AnyConnect is installed many customers still prefer to train their end-users to log in using a web-browser. This permits the administrator to include messaging to the end user, include bookmarks to resources or provide other features to the end-user. This works very well for organizations that utilize the Clientless SSL VPN features of the Cisco ASA. Many organizations find that network access is not, in fact, required for their employees to remain productive and have access to essential resources. This has the additional benefit of keeping the remote computer ‘at arms length’; remote access clients are not connected to the network, but instead are accessing resources through the secure portal.

When AnyConnect is required several options are available. The administrator can choose to have end-users invoke the AnyConnect client from the portal, logging in to the portal can automatically start the AnyConnect client, or end-users can learn how to launch the AnyConnect application and log in to the VPN without using a web-browser.

AnyConnect, launched stand-alone as an application, provides features that can assist with the re-enrollment process, when an end-user’s certificate is expiring. The AnyConnect client can be configured to provide notifications to the end-user that their certificate is approaching the end of its lifetime, and once expired, the ASA can provide a message to the end user instructing them to open a browser to the SSL VPN URL.

As with access from a browser, the username is pre-filled from the certificate and the end-user is prompted to enter their password to authenticate to the VPN for network access to corporate resources.

Once the end-user has authenticated with a valid certificate plus password no other action is required.
When the certificate is approaching the end of its lifetime AnyConnect can be configured to warn the end-user.

Once the certificate has expired the ASA can be configure to provide the end-user with information and instructions how to re-enroll for a valid certificate so that they can continue to authenticate to the VPN directly from the AnyConnect client.
Cisco VPN Client (IPSec Client) Integration

The IPSec client was recently declared End-of-Life by Cisco system (as of March 2013). This means Cisco will not be publishing updates to the client after 2014 and will eventually stop supporting the client altogether.

Many customers already using the IPSec client will opt to continue using it for a period of time, though.

SecureAuth IdP supports some very unique features to make the IPSec client easier to use when a token-less two-factor authentication model is desired. The enrollment process is exactly the same; the end-user must open a browser and point to the SecureAuth server in order to obtain a valid certificate to be used for secure remote access.

SecureAuth IdP not only creates and installs a certificate, SecureAuth IdP also will automatically, and transparently to the end-user, modify the connection profile for the IPSec client to use the certificate for authentication.

When the certificate is nearing expiration the VPN Client will provide a notification to the end-user of the impending expiration. This message cannot be customized within the client.

When the certificate has expired, a somewhat less friendly message, that is also not configurable, will be displayed to the end-user, and the enterprise will have to depend on end-user training to direct the end-user to SecureAuth IdP to obtain a valid credential.

When everything goes right with the IPSec client the experience is much more friendly.

The IPSec client will automatically send the valid certificate to the Cisco ASA. Again, SecureAuth IdP integration often relies on an ASA feature called Certificate to Profile Maps to deliver the end-user’s session to the correct connection profile in the ASA configuration.

To the end-user it appears, as it always had, that all that is required is to click on the Connect button, and type in the password.
Summary

SecureAuth IdP supports all of the secure remote access features that Cisco has available in the Cisco ASA.

The Clientless SSL VPN and the AnyConnect integration paths, that utilize the newest and most feature rich remote access solutions offered by Cisco, are among the most popular and easiest to support. But, for organizations not yet ready to migrate away from the IPSec client, SecureAuth offers an immediate solution to a two-factor authentication need.

SecureAuth IdP offers the best two-factor solution for assuring identity and network integrity, and offers a path to migrate to the newest Cisco VPN features with a tightly integrated, simple to use and easy to support authentication solution.