

MultiFactor SecureAuth® Facilitates a Secure Migration from Cisco IPSec to Cisco SSL VPN Remote Access

One of the vexing issues facing enterprises today – is how to realize the administrative cost savings and increase user functionality of Cisco’s ASA SSL VPN offering. The user advantages of SSL VPN have been documented and discussed, and thus this article will not delve into the “why’s” of SSL VPN deployments.

The key issue, has been, how to implement a solution:

1. That facilitates the transition TO a “SSL VPN” solution FROM a tradition IPSec-based solution.
2. Ensures Secure User Authentication in the process – that is port a secure authentication for the present IPSec clients to the new SSL VPN base.
3. Is deployable to both the enterprise and end user

MultiFactor SecureAuth® provides such a solution.

Step #1 – Original State, Non-X.509 Authentication for the Cisco IPSec VPN

Let’s start with the initial state, Diagram #1, IPSec VPN tunneling via the Cisco IPSec client and a Cisco IPSec supporting appliance (VPN 3000 Concentrator, PIX Firewall, Cisco Routers, etc).

Step #1: Original State, Non-X.509 Authentication via Cisco IPSec VPN

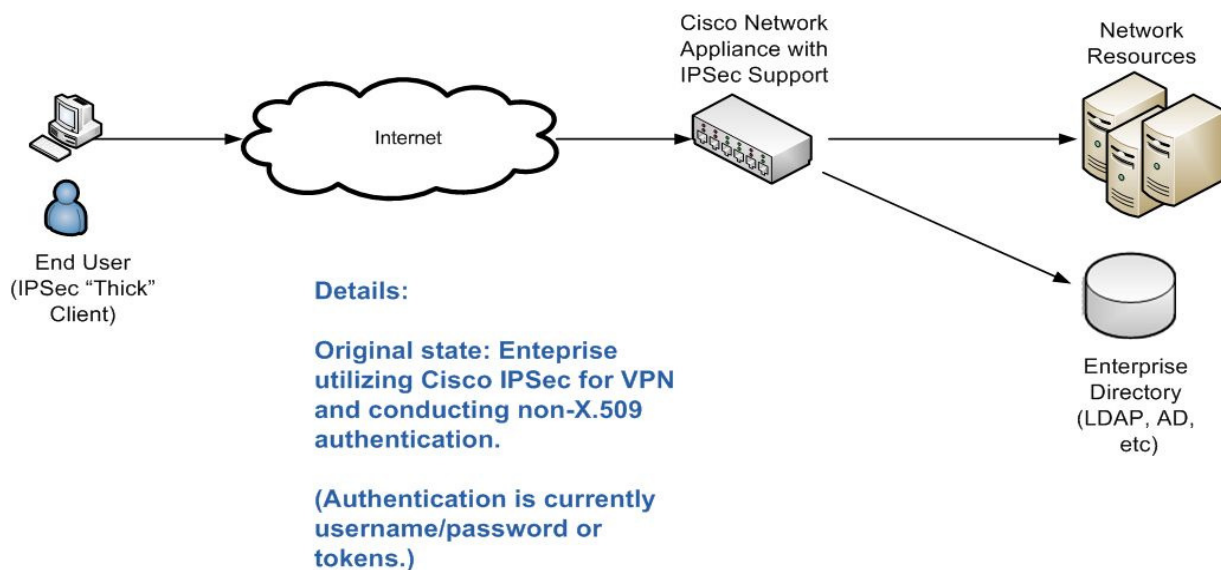


Diagram #1 – Original State: An IPSec User VPN Deployment

In the original state, the user is deployed with a Cisco IPSec client and is utilizing authentication other than secure X.509 bilateral authentication.

In addition to the authentication being insecure – the organization is also at risk with a “Shared Authentication” key being utilized for encryption. This means that even if the organization is utilizing tokens (hard or soft) for authentication – the encryption is still a mere password – and thus vulnerable to attack. **(See Diagram #2)**

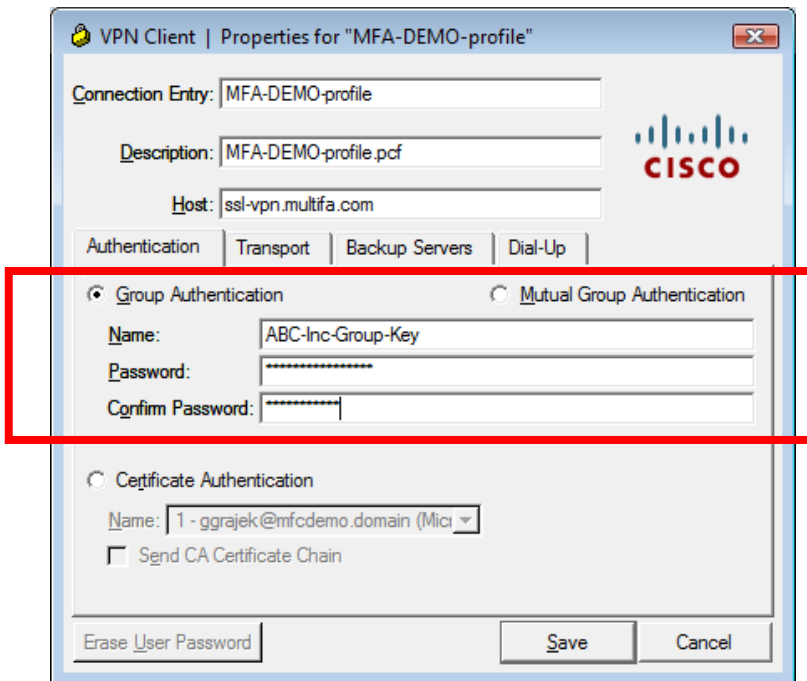


Diagram #2 - IPSec Client Configured to use a shared “Group Authentication” key

Step #2 – Secure X.509 Authentication/Encryption to Cisco IPsec via SecureAuth®

The next step in this scenario is to:

1. Add a Cisco ASA and a MultiFactor SecureAuth appliance into the enterprise
2. Utilize SecureAuth to enroll users with X.509 Certificates and a new user IPsec profile
3. Enable X.509 Authentication on the Cisco IPsec appliance with the new certificates and user profiles.

(See Diagram #3)

- Step #2. A) User X.509 Enrollment via Cisco ASA SSL VPN/SecureAuth Deployment
 B) SecureAuth Updates User's profile for X.509 Credential
 C) Cisco IPsec Authentication/Encryption via SecureAuth X.509 Credential**

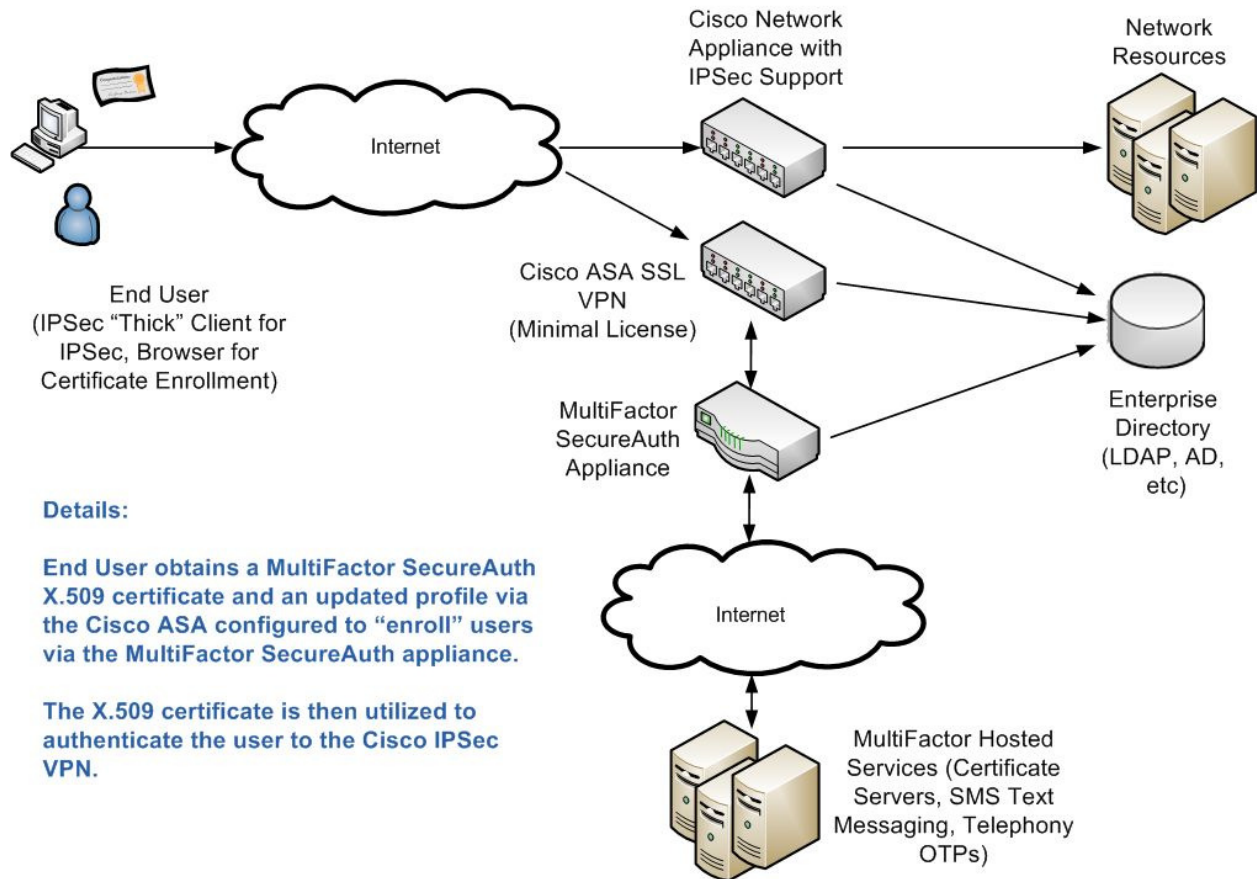


Diagram #3 – Utilizing the Cisco ASA/SecureAuth® solution to distribute X.509 Credentials and new IPsec Profiles.

In this step, the enterprise deploys new X.509 credentials and new IPSec user profiles via the MultiFactor SecureAuth appliance. One of the advantages here – is that the enterprise, at this time, does not need purchase a large Cisco ASA SSL VPN license – a simple 2 to 25 user license – will suffice. The enterprise simply utilizes the ASA for the deployment of SecureAuth X.509 credentials and new IPSec user profiles.

The MultiFactor SecureAuth® appliance is designed to plug into the enterprise in a matter of hours. The “rocket science” of Certificate creation, SMS Text Messages and Telephony OTPs is handled via secure and world-unique set of MultiFactor-hosted, WSE 3.0 Web Services.

In addition to the user now being secured via valid X.509, bilateral authentication – SecureAuth® also creates a new user profile for the user that utilizing the new X.509 credential. **(See Diagram #4.)**

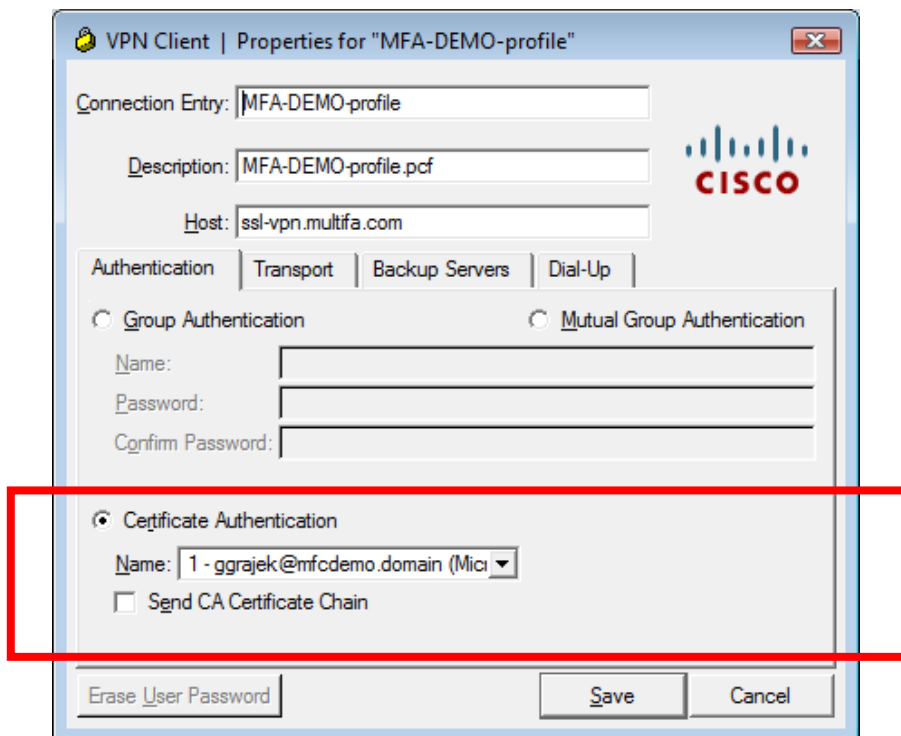


Diagram #4 – New User profile deployed by SecureAuth via User-Self enrollment. Note the usage of the X.509 certificate for encryption.

It is important to note – that the end state of this step – is that the user is now conducting secure bilateral X.509 authentication AND encryption to the Cisco IPSec. This is a vast security improvement over both username/password and one-time-passwords.

Step #3 – SecureAuth X.509 Authentication to the Cisco ASA SSL VPN

In this step the enterprise switches from an IPSec deployment to a full SSL VPN deployment. The same URL that was utilized to deploy the SecureAuth X.509 credential – can now be utilized for the Cisco ASA SSL VPN connection. In addition, the same X.509 credential issued by SecureAuth in Step #2 above, is utilized for the Cisco ASA SSL VPN authentication. **(See Diagram #5)**

Of course, for the ASA SSL VPN roll-out in this step, a larger Cisco ASA SSL VPN license is needed to handle the concurrent connections. But the advantage is, now users no longer need to have the Cisco IPSec client and profiles on their machines to connect. And because the SSL VPN authentication is through SecureAuth’s secure X.509 registration system, which can utilize both SMS Text Messaging and Telephony OTPs for registration – the enterprise can be assured that the SSL VPN users are verified.

Step #3. User Authenticates to Cisco ASA SSL VPN with SecureAuth X.509 Credential

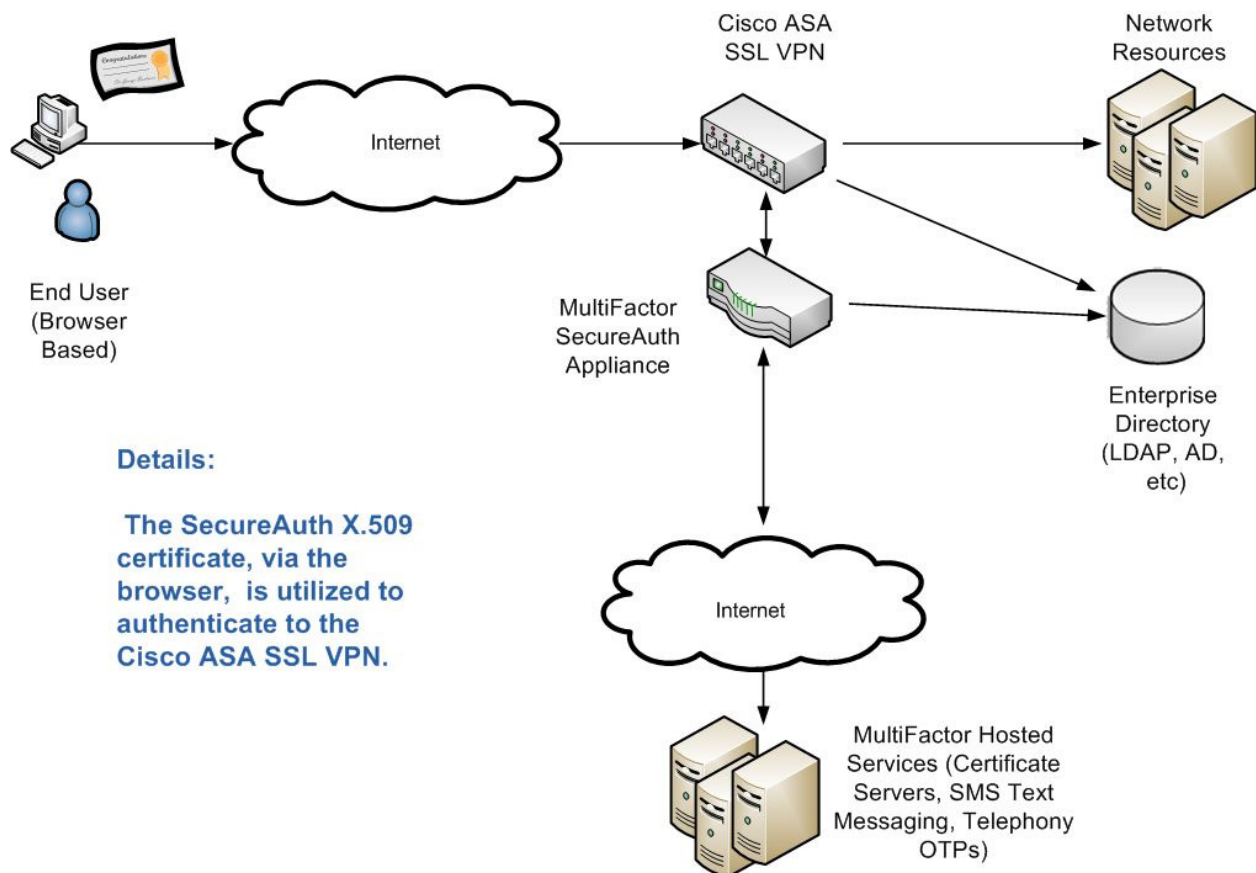


Diagram #5 – SecureAuth X.509 Authentication to the Cisco ASA SSL VPN



Summary:

Enterprises have been searching for a methodology to migrate from tradition IPsec VPNs to the nimbler and more-user friendly SSL VPN solutions. The SecureAuth authentication system provides this solution that is:

- Secure
- Deployable
- And User and Enterprise “friendly”