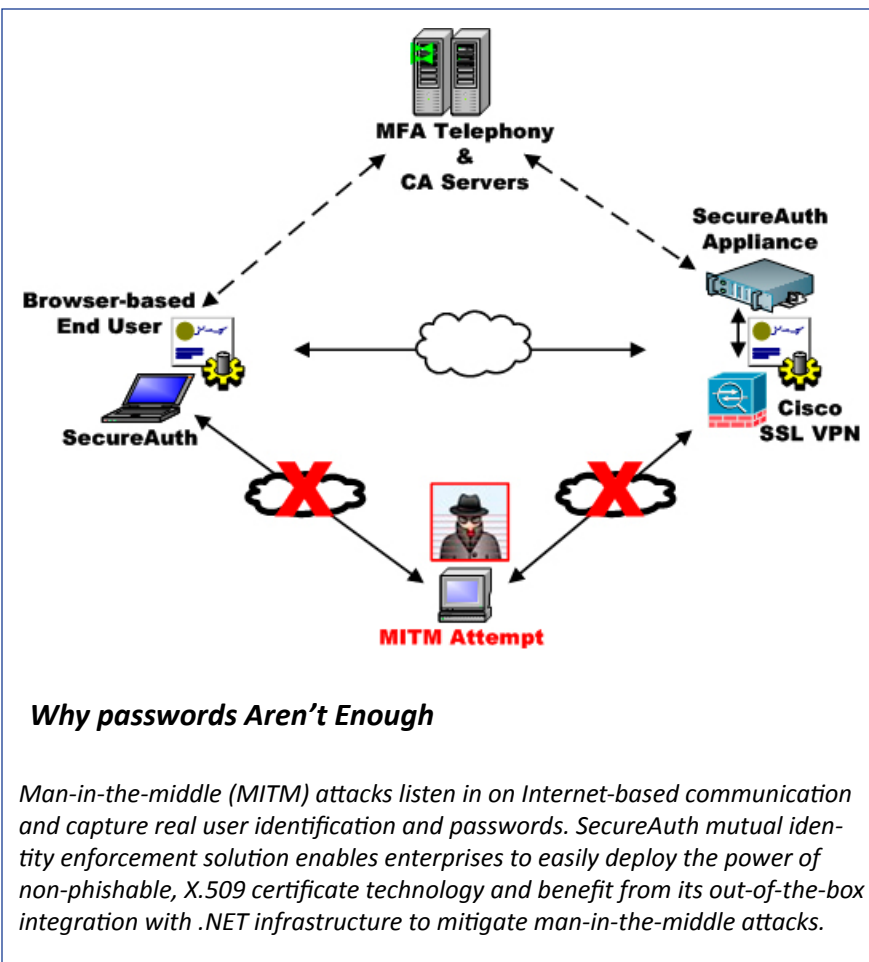




SecureAuth™ for Cisco® ASA SSL VPN

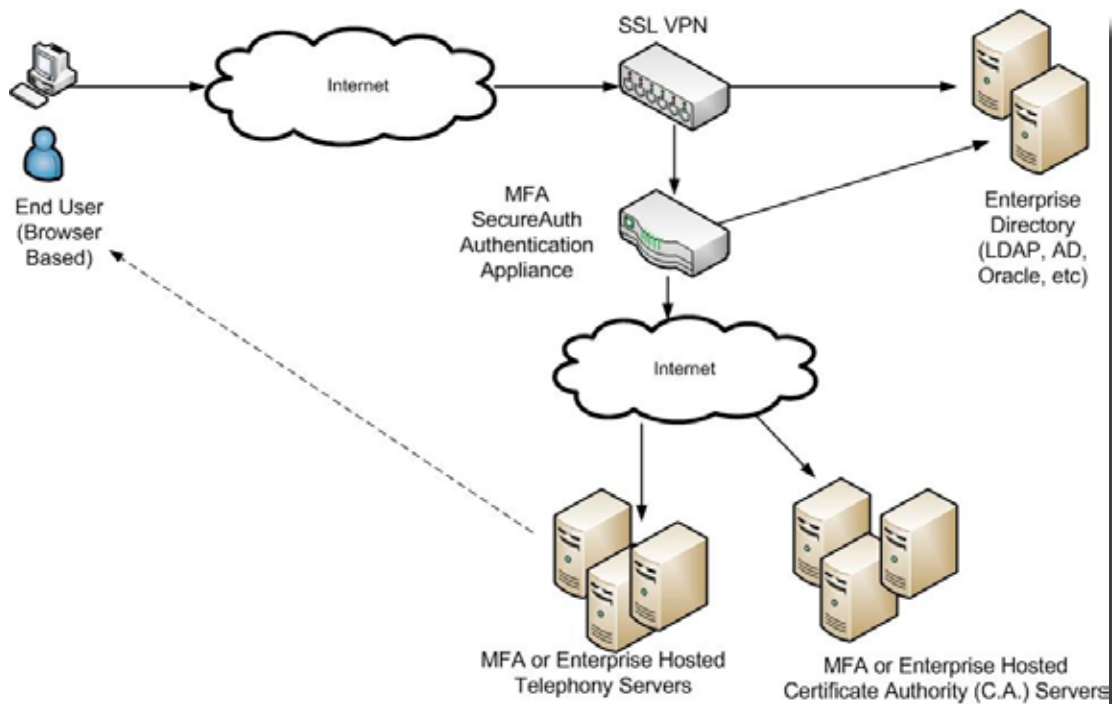
Strong, Two-Factor Authentication Meets the Manageability of SSL VPN

SecureAuth™ for the Cisco Adaptive Security Appliance (ASA) SSL VPN is the only tokenless, non-phishable authentication solution for SSL VPNs that mutually authenticates both the user and the server, in an easy to deploy manner. Using a combination of a hardened appliance and web services, SecureAuth integrates tightly with the Cisco ASA SSL VPN to provide a turnkey solution to deliver an algorithmically proven method that thwarts man-in-the-middle phishing attacks. Residing in the enterprise network and using existing data stores such as Active Directory, the SecureAuth solution features out-of-band self-registration and automatically delivers X.509 certificates seamlessly to end users. The solution eliminates the need for administrator resources to deploy software, install upgrades or train end users on complex remote access procedures.



Distinctive Features

- Out-of-the-box integration to Cisco ASA SSL VPN for same day deployment with full X.509 level user authentication
- Integrates with existing data store, such as Microsoft Active Directory (LDAP)
- Out-of-band registration (telephony or SMS) to prevent man-in-the-middle exploits
- No tokens, data servers or additional infrastructure investment required
- No private enterprise information stored in the hosted SecureAuth infrastructure
- Eliminates need for administrator to deploy and upgrade end-user software
- User friendly self-registration and automated certificate distribution reduces help desk calls
- Full Firefox browser support



SecureAuth System Architecture and Work Flow

1. The SecureAuth plug-and-play appliance is deployed in the enterprise's private network.
2. An end-user initiates an access request to the Cisco ASA SSL VPN. (If a user does not have an X.509 v3 personal certificate, the user is redirected to the SecureAuth appliance.)
3. SecureAuth coordinates user authentication between the end-user and the enterprise's existing authentication scheme (e.g., username/password checking). Using the SecureAuth telephony web service or short message service (SMS), a randomly generated, one-time password (OTP), SecureAuth strengthens the end-user registration process and mitigates phishing attacks during this process.
4. Upon successful end-user authentication, SecureAuth automatically installs the X.509 certificate on the end-user's device, if none exists.
5. Authenticated users can securely access the enterprise resources and applications appropriate to their roles.
6. On subsequent access requests, Cisco ASA SSL VPN retrieves the SecureAuth-generated certificate from the end-user's device and authenticates it without the need to re-initialize and re-register the users. They simply use their enterprise network user name and password, and a full bi-directional, non-phishable authentication automatically takes place for each new access request.