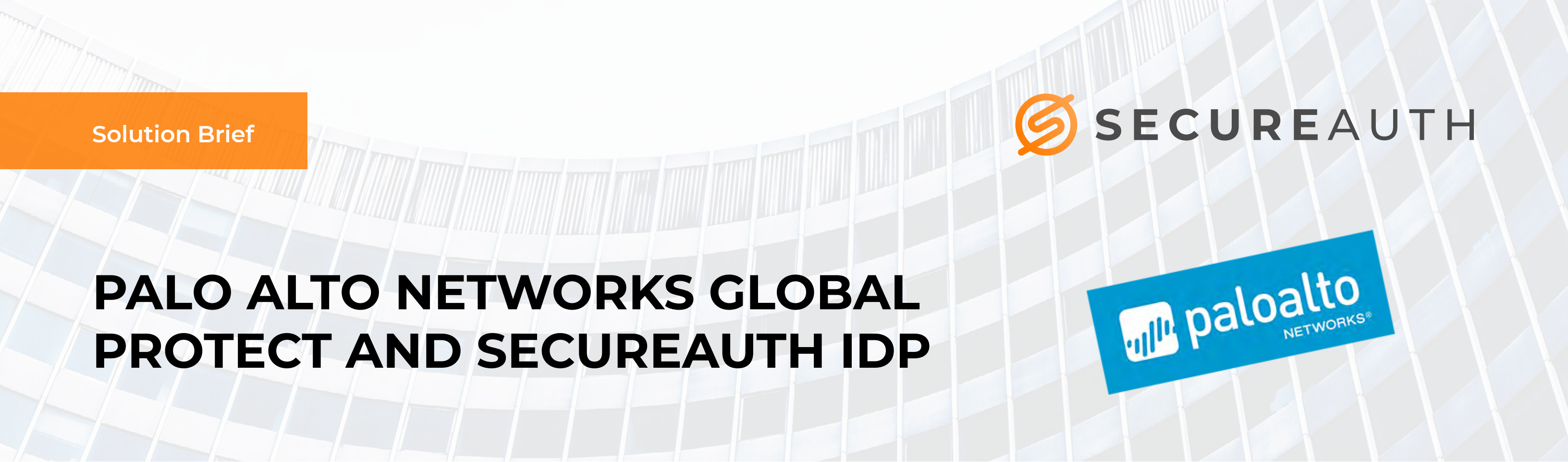


Solution Brief

PALO ALTO NETWORKS GLOBAL PROTECT AND SECUREAUTH IDP

Unprecedented protection against today's sophisticated attacks

SecureAuth integrates with Palo Alto Networks GlobalProtect to provide an advanced user authentication solution that goes beyond simple-two-factor to determine identities with confidence. SecureAuth IdP analyzes multiple factors to determine the legitimacy of every login attempt, thwart attacks in-process and render compromised credentials worthless.

Palo Alto Networks GlobalProtect provides an SSL VPN connection that insures that your network has a secure connection via the remote access tunnel insuring that all your sensitive data is protected along the pathway. Palo Alto Networks integrates with SecureAuth via its Radius Server and Threat Service in a matter of minutes.

In PAN-OS v7, a new feature includes a RADIUS attribute containing the client IP address which lets SecureAuth IdP/RADIUS server execute Adaptive Authentication workflows for users logging on via the GlobalProtect VPN client. Based on the client IP address, SecureAuth IdP can use Geo-location, Geo-velocity, and Threat Service analyses in these workflows which range from completely denying an authentication request if the client IP is originating from a blacklisted IP/Country, to stepping up the authentication request if a Geo-velocity violation is detected.

Solution Highlights

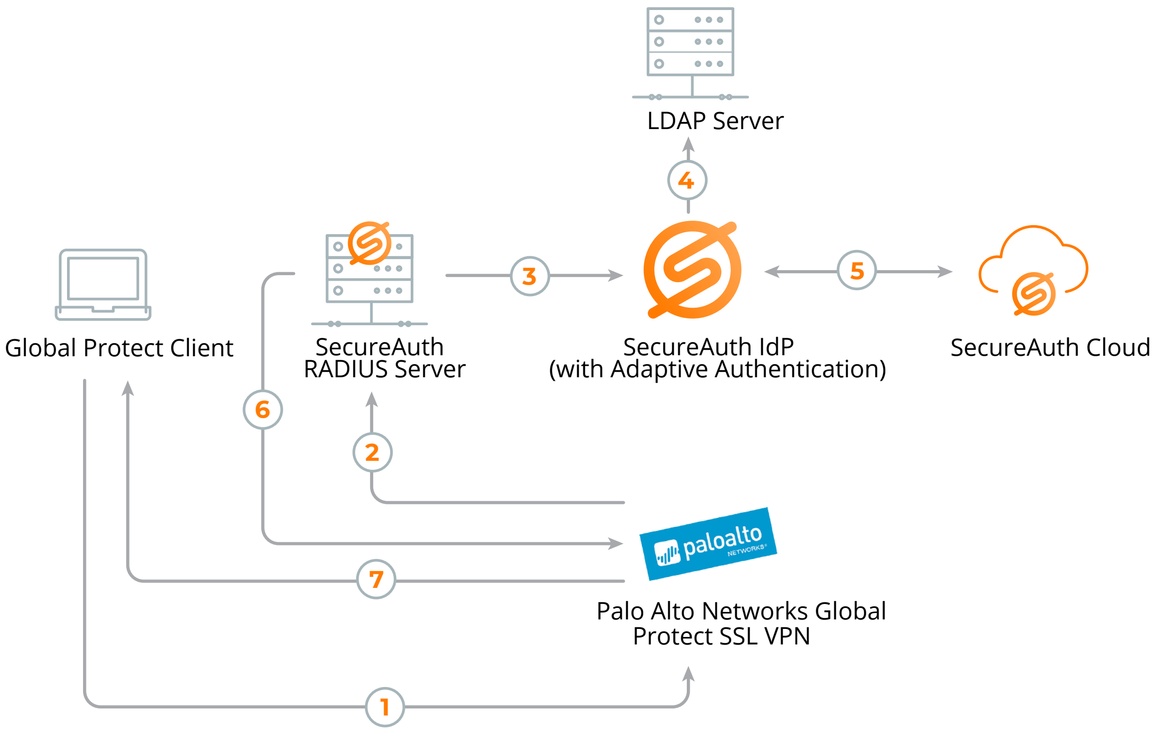
+ **Improved Protection**
  Identifies today's advanced threats using the SecureAuth Threat Service and Palo Alto Networks GlobalProtect.
+ **SecureAuth Attribution data**
  Provides context around the IP address, such as actor type and malware family
+ **Greatest coverage**
  Combines multiple industry-leading threat data from Palo Alto Networks and SecureAuth
+ **No user disruption**
  Maintains a smooth user experience by requiring multi-factor authentication only when risks are present
+ **25+ authentication methods**
  Options include SMS, telephony, email one-time passwords (OTPs), push-to-accept, symbol-to-accept and USB keys

Moving beyond simple Two-Factor Authentication

SecureAuth's adaptive authentication workflows to determine identities with absolute confidence and ensure that only the valid users get access to corporate resources. By integrating with the SecureAuth Radius Server, Palo Alto Networks customers can go beyond simple two-factor with pre- authentication risk analysis including inspection of IP address, geo-location, device recognition and more.

Detect and Respond to Advanced Threats

Attackers can re-use compromised credentials to gain access to internal corporate resources. By utilizing the SecureAuth Radius Server and SecureAuth Threat Service, Palo Alto Networks GlobalProtect customers can better secure corporate resources. When the SecureAuth Radius Server, utilizing the Threat Service, detects a GlobalProtect client attempting to log in, it assesses the risk associated with the access attempt and then either allows access, denies access, or requires multi-factor authentication. This approach streamlines access for legitimate users while stopping attackers cold.



1. A user opens the Palo Alto Networks GlobalProtect VPN Client and enters a username and password; the user's details are sent to Palo Alto Networks GlobalProtect

2. The Palo Alto Networks GlobalProtect VPN server acts as a RADIUS client and sends RADIUS authentication details along with the user's credentials to the SecureAuth RADIUS server.

3. Upon RADIUS authentication approval, SecureAuth RADIUS sends user credentials to SecureAuth IdP via an API call.

4. SecureAuth IdP authenticates the user's credentials using the LDAP server as a first factor authentication.

5. Upon successful LDAP authentication, the SecureAuth RADIUS server initiates the second factor workflow. Another API call is invoked to SecureAuth IdP to validate against Adaptive Authentication rules and violations. SecureAuth IdP sends the client IP address obtained by SecureAuth RADIUS server to SecureAuth Cloud where it is analyzed for Geo-location, Geo-velocity, and Threat Service violations.

6. The RADIUS server returns a response to the Palo Alto Networks GlobalProtect VPN. If a violation occurs, one of the following actions can be taken: Hard stop, Redirect, Step-up authentication, Step down authentication, Resume authentication, or Post authentication. If Step-up authentication is selected, 6 methods of 2-Factor Authentication are available: TOTP, P2A, OTP, SMS, VOICE, EMAIL.

7. The GlobalProtect VPN client shows the specified workflow for the Adaptive Authentication event.

About SecureAuth

SecureAuth empowers organizations to determine identities with confidence. SecureAuth IdP provides authentication security, single sign-on, and user self-service tools together in a single platform, enabling strong identity security while minimizing disruption for legitimate users.

Learn more at www.secureauth.com

About Palo Alto Networks

Palo Alto Networks is a next-generation security company that is leading a new era in cybersecurity by safely enabling applications and preventing cyber breaches for tens of thousands of organizations worldwide. Built with an innovative approach and highly differentiated cyberthreat prevention capabilities, its game-changing security platform delivers security far superior to legacy or point products, safely enables daily business operations, and protects an organization's most valuable assets. Find out more at www.paloaltonetworks.com.