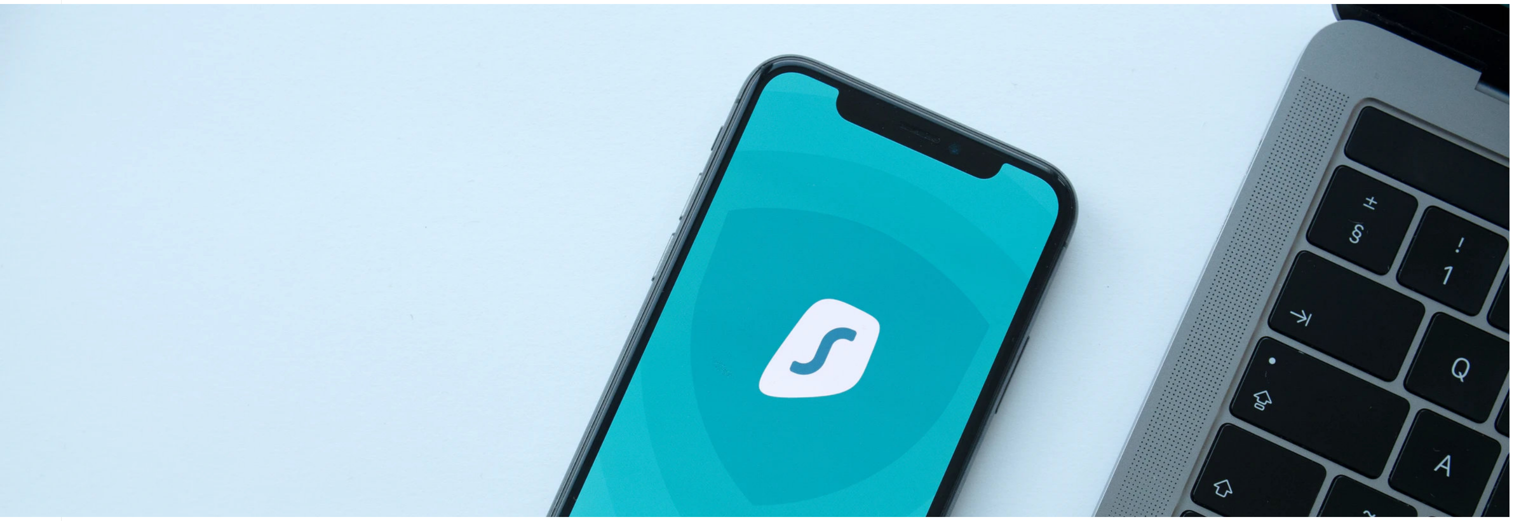
next-gen wired & wireless security



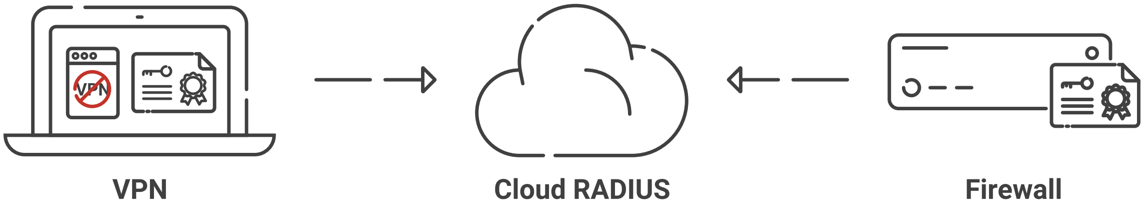
Certificate-based Authentication for VPN

The strengths of VPN are also its weaknesses: the encrypted tunnel does a great job at protecting your traffic from prying eyes, but it also prevents IT from being able to accurately monitor network usage.

Using **X.509 digital certificates** to authenticate to VPN enhances the security of the connection while providing more identity context about who or what is using the network, as well as offering expanded options for policy enforcement (such as restricting access to corporate devices).

Although wireless controllers universally support EAP-TLS (or client certificate-based authentication) for 802.1X, this is not the case for VPNs. It's an unfortunately common oversight, but many VPN vendors don't natively support EAP-TLS.

If Your VPN Does Not Support EAP-TLS



SecureW2's Cloud RADIUS is built primarily for client certificate authentication via EAP-TLS, but we have solutions that enable us to support almost any VPN:

- Azure MFA - VPN Integration - Authenticate VPN using Azure's MFA service in lieu of a RADIUS server. This method can be configured to enable conditional access policies and to generate RADIUS-like accounting logs.
    - (Alternatively, we can use an Azure MFA license in combination with our Cloud RADIUS to perform SAML authentication, issue a unique username and password to your VPN, and trigger the Microsoft Authenticator App automatically to authenticate the session.)
- SecureW2's Managed PKI - Accomplish certificate-based authentication by integrating our Certificate Authorities into your firewall to establish a chain of trust.

Once set up, you'll be able to use our **APIs for certificate management** - regardless of the VPNs compatibility. Enforce role-based access policies, access analytics and reporting tools, and automate the certificate lifecycle (including auto-revocation) all from one place.

Example Configuration Guide

To give you an idea of the configuration process, here is our integration documentation for Palo Alto's GlobalProtect. It's a good reference for how our CAs are set up so that authentication happens on the firewall.

Read Documentation

Preparatory Questions

In order to facilitate our conversation, we'll need a few key pieces of information from you about your organization and your network. Answering these early on can spare us from some lengthy emails and ensures we can address the most relevant questions over a quick call.

1. Do you have an **existing VPN** or a potential VPN already in mind?
2. How is your network currently secured? Do you already use a **RADIUS** server?
3. **How many end-user devices** do you have on your network?

Frequently Asked Questions

- Do you support X VPN?
    - All of our products are vendor neutral, so the answer is typically "yes".
- Does SecureW2 have a minimum device requirement?
    - We work with small to enterprise level companies. Please let us know if you would like to purchase through a partner channel.
- Does SecureW2 serve X vertical?
    - We have customers of all shapes and sizes in every vertical - including many international accounts.
- What is the cost per device?
    - Price is per end-user device with at least one valid client certificate from our PKI. Multiple certificates on one device is still priced at one device. Infrastructure with certificates, such as a server with an SSL certificate, is priced the same. Infrastructure without client certificates, such as access points, are included gratis