Hardware Token Authentication

https://campus.barracuda.com/doc/39813185/

Two factor or multi-factor authentication is considered to be strong authentication because it requires two factors:

- Something only the user knows (e.g., password)
- Something only the user has (e.g., mobile phone)

For the Barracuda SSL VPN, hardware solutions are based on two different authentication mechanisms: the RADIUS and the SSL Client Certificate authentication modules.

Hardware token authentication using SSL client certificates

The token or smart card contains an SSL client certificate which is used to authenticate to the system. Some vendors require software installed on the client or card readers, depending on the solution.

- SafeNet iKey 2032
- Aladdin eToken PRO

SafeNet iKey

The SafeNet iKey uses a small USB device that is typically carried on a key chain by users. It uses SSL client certificates to present a certificate to the Barracuda SSL VPN. For more security, users must also enter a secret passphrase. The client computer must have a special utility (CIP) installed, which uploads the certificate on the USB token to the Windows certificate store. The browser then uses this certificate when authenticating to the Barracuda SSL VPN.

Aladdin eToken PRO

Similar to the SafeNet iKey, the Aladdin eToken uses an SSL client certificate to authenticate. It also uses special software that must be manually installed on every client computer.

Hardware token authentication using RADIUS integration

Other hardware token authentication servers use a built-in or external RADIUS server. The Barracuda SSL VPN queries the RADIUS server as a part of its multi-factor authentication process, allowing the use of OTP and CryptoCard tokens.

- RSA SecurID
- VASCO Digipass Token
- Secure Computing Safeword

RSA SecurID

RSA SecurID uses its built-in RADIUS server to enable communication between the appliance and the RSA server. With an Active Directory user database, using RSA SecurID is especially powerful because you can centrally manage the account with both the appliance and RSA Authentication Manager reading accounts from your Active Directory domain.

For more information, download the RSA SecurID Ready Implementation Guide (PDF).

VASCO Digipass

A VASCO server can authenticate with the Barracuda SSL VPN via an external RADIUS server. The VASCO server currently does not include a RADIUS server.

Secure Computing Safeword

Safeword servers include a RADIUS feature that can be used to authenticate to the Barracuda SSL VPN. Note that Safeword requires an Active Directory database and Internet Authentication Server (IAS) installed on the domain controller.