ZYXEL
NETWORKS

SecuExtender

IPSec VPN Client Subscription Service

Software Release Note

For macOS
Version 1.2.0.7

May 13, 2021

System Requirement

- macOS 10.15 or above
- The macOS version software must be activated with a license key from SecuExtender IPSec VPN Client Subscription Service for Windows/macOS (1YR/3YR license)
- The software is NOT compatible with the license key from legacy SecuExtender IPSec VPN Windows Client (perpetual license)
- 30 days trial is supported
- 15 days grace period is supported

New features, improvements, and fixes of release 1.2.0.7

- Feature: The macOS version software is now distributed as a DMG installer through Zyxel web site
- Feature: Compatible with Zyxel firewalls USG FLEX/ATP/VPN/USG/ZyWALL series, and virtually all existing IPsec IKEv2 compliant gateways
- Feature: AES CBC 128/192/256 encryption
- Feature: DH Group support (19-21 Elliptic Curves)
    a. Group 14: MODP 2048
    b. Group 15: MODP 3072
    c. Group 16: MODP 4096
    d. Group 17: MODP 6144
    e. Group 18: MODP 8192
    f. Group 19: ECP 256 (IKEv2 only)
    g. Group 20: ECP 384 (IKEv2 only)
    h. Group 21: ECP 512 (IKEv2 only)
- Feature: Authentication supports PSK, Certificates, EAP (IKEv2 only)
- Feature: Redundant Gateway, DPD
- Feature: Mode Config (auto, manual)
- Feature: Gateway Certificate Authorities (CA) can now be imported into the VPN Client

- Feature: Ability to force the VPN Client to open a tunnel only if the gateway CAs are valid
- Feature: Added Get From Server" menu item to retrieve VPN configurations remotely
- Feature: retrieve VPN configuration from gateway
- Feature: EAP pop up for authentication
- Improvement: support of request for "mode-cfg type 3" to receive DNS from gateway

Design Limitation

1. The macOS version software does not support adding up multiple time-based license keys. Please activate the software with ONE license key, before it is being expired.

2. The macOS version software discontinues the support for IKEv1

3. Discontinuing support for weak ciphers:
- IKEv1: DES, 3DES, MD5, SHA1, DH1, DH2, DH5
- IKEv2: DES, 3DES, MD5, SHA1, DH1, DH2, DH5, and NoDH for Ike Child
- If the configuration on the gateway side uses one of the removed algorithms, then the client will not connect

4. The following ZyWALL/USG VPN Gateway rules configured cannot be provisioned to the SecuExtender IPSec VPN Client for macOS:
- Multiple Authentication not applicable
- Gina mode cannot function in occasions where VPN rules are moved to USB drive
- VPN Client Address will be void in occasions where the Client and the Gateway are not unanimously both IPv4/IPv6, and users will be notified that "VPN Client Address is void so tunnels cannot be built with success"
- IPv4 rules with User-based PSK authentication