ZYXEL NETWORKS

SecuExtender

Zero Trust IPSec/SSL VPN Client

Never Trust and Always Verify

Businesses from small to large all need to get ready for the growing demands of an increasingly mobile workforce and distributed work site expansions. As to protect your businesses from inside out, you need the right VPN service to apply proper access control.

Zero-Trust Network Security

VPN management consolidates and ensures the same network control and security across multiple sites. We extend the working experience easily and securely, as if you were in the office with the safety of both two-factor authentication and tunnel protection. Our SecuExtender VPN Client gains to a Zero-Trust Network Security, gives you a flexibly easy-to-use, simple-to-deploy Virtual Private Network (VPN) solution that provides roaming users with secure, performance and reliable remote access back to office network.

- Secure and reliable remote access, preserving business operations and data integrity
- Supports both IPSec/SSL VPN and secure authentication methods
- Simple to deploy with remote VPN wizard
- Runs on both Windows and macOS operating systems

Datasheet SecuExtender

Secure Access to the Office Network Anywhere

The SecuExtender VPN Client is designed with an easy 3-step configuration wizard to help employees create remote VPN connections quicker than ever. The VPN configurations and security elements including pre-shared key and certificates, can be retrieved directly from a Zyxel firewall. Users can easily access their remote applications and data as if they were in the office.

A Secure, Flexible All-round VPN Client Subscription

The new time-based subscription allows you to customize the solution according to your specific business requirements. This versatile client supports your remote workforce, granting you the flexibility to access your network securely from any location outside the office. Whether you're working in the office or from a home office, this VPN service prioritizes security, ensuring peace of mind as you communicate over the Internet. It provides one of the best methods to safeguard your privacy and protect sensitive information during online interactions.

Secure Remote Access

- Ensure secure and reliable data transmission
- Support Two-factor authentication (2FA) for strengthen protection*
- Added stronger key exchange (DH) group and algorithms

Enhanced Usability

- Windows and macOS operating system supported
- Flexible subscription plan and easy to renew/purchase online
- Immediate access to all latest updates and future releases

Simple Deployment

- Easy-to-use remote VPN wizard (IKEv2 preferred)
- 1-click provisioning by downloading VPN settings directly from a Zyxel firewall
- Easily choose IPSec VPN or SSL VPN to meet your needs
- Intuitive panel with 25 multilingual support

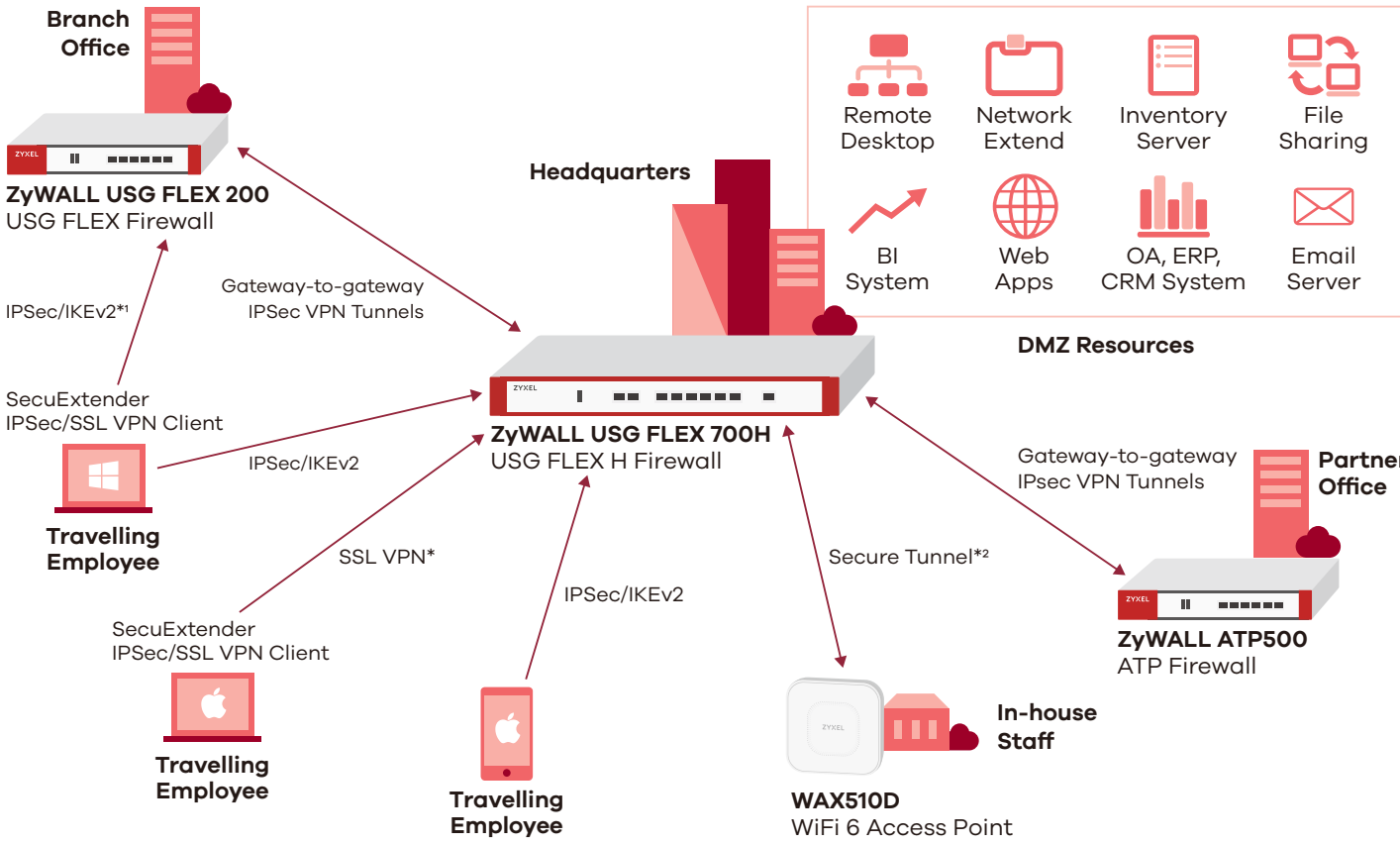
*: Two-factor authentication (2FA) is only supported in Windows version, not supported in macOS version. SecuExtender 2FA is compatible with Zyxel firewalls from the USG FLEX/ATP/VPN series. The USG series does not currently support 2FA.

Remote Access Security Solutions

Operating with Zero Trust best practices across wired or wireless network infrastructures – wherever your employees: HQ, branch offices, on-the-go, or even working from home. Together we can help your business maintain continuity and safety.

Secure Workplace	Remote Access Solution	Benefits
Working on the go for teleworkers	SecuExtender VPN Client	• Secure access with reliable IPSec/SSL VPN connectivity • Easy installation and simple user experience • Cost-effective subscription service • Two-factor authentication (2FA)
Home offices	Remote Access Point (RAP)	• Layer 2 extension with synchronized security • Simple provisioning • Two-factor authentication (2FA)
Remote location between HQ & branch offices	ZyWALL USG FLEX Series Firewall	• Advanced protection with central management • Secure encrypted tunnel • Two-factor authentication (2FA)

Application Diagram



*: SecuExtender IPSec/SSL VPN Client now supports connecting to USG FLEX H series using an SSL VPN tunnel.
*1: When connecting the SecuExtender IPSec/SSL VPN Client to a USG FLEX or ATP firewall, you can only use the IPSec/IKEv2 protocol because SSL VPN is not supported in this combination.
*2: Available in Q2, 2024.

SecuExtender Zero Trust IPSec/SSL VPN Client Subscription

System specifications

- Windows 10, Windows 11 (64-bit)
- macOS 10.15 or above

Hardware specifications

- 1 GHz x86-64 processor
- RAM: 2 GB
- 40 MB available disk space

Product specifications

Hash Algorithms
- SHA2-HMAC 256-bit authentication
- SHA2-HMAC 384-bit authentication
- SHA2-HMAC 512-bit authentication

Encryption
- AES 128, 192, 256-bit encryption
- AES GCM 128, 192, 256-bit encryption
- AES CTR 128, 192, 256-bit encryption

Diffie Hellman Group Support
- Group 14: MODP 2048
- Group 15: MODP 3072
- Group 16: MODP 4096
- Group 17: MODP 6144
- Group 18: MODP 8192
- Group 19: ECP 256 (IKEv2 only)
- Group 20: ECP 384 (IKEv2 only)
- Group 21: ECP 512 (IKEv2 only)

Diffie-Hellman Key Group Support
- DH28: BrainpoolP256r1 ECC [RFC 5639]

Authentication Mechanism
- PSK (Pre-shared Key)
- EAP (Login/Password)
- PKCS #11 Certificate
- Supports frequencies:
  - Method 1: RSA Digital Signature with SHA-2 [RFC 7296]
  - Method 9: ECDSA "secp256r1" with SHA-2 (256 bits) on the P-256 curve [RFC 4754]
  - Method 10: ECDSA "secp384r1" with SHA-2 (384 bits) on the P-384 curve [RFC 4754]
  - Method 11: ECDSA "secp521r1" with SHA-2 (512 bits) on the P-521 curve [RFC 4754]
  - Method 14: Digital Signature RSAS SA-PSS and RSASSA-PKCS1-v1_5 with SHA-2 (256/384/512 bits) [RFC 7427]

X.509 Certificate Management
- PSK (Pre-shared Key)
- EAP (Login/Password)

IKEv1
- End of support for the vulnerable IPSec/IKEv1 protocol, which has been deprecated by the IETF in September 2019
- End of support for vulnerable algorithms DES, 3DES, SHA-1, DH 1, DH 2, DH 5 in IPSec/IKEv2 (even in "auto" mode)

IKEv2 Support
- Mode CP
- IP fragmentation
- NAT-Traversal
- Childless IKE (RFC 6023)
- Extended Sequence Number (ESC) (RFC 4304) IPSec/IKEv2 (even in "auto" mode)

Endpoint Visibility
- Collecting endpoint information admission control
  - MAC addres
  - Inner IPv4 address
  - Hostname
  - Unique ID
  - Zyxel client version
  - OS type
  - OS version
  - System manufacturer
  - System model

Networking
- NAT traversal (Draft 1, 2 & 3)
- Dead Peer Detection (DPD)
- Redundant gateway

Connection Technologies
- Dial-up modem
- GPRS
- Ethernet
- WiFi

SSL VPN[*1]
- TLS Requirements
  - TLS 1.2 Medium
  - TLS 1.2 High
  - TLS 1.3
- Hash Algorithms
  - SHA2-HMAC 224-bit authentication
  - SHA2-HMAC 256-bit authentication
  - SHA2-HMAC 384-bit authentication
  - SHA2-HMAC 512-bit authentication
- Encryption
  - AES CBC 128-bit encryption
  - AES CBC 192-bit encryption
  - AES CBC 256-bit encryption
- Authentication Mechanism
  - PSK (Pre shared key)
  - EAP (Login/Password)
  - PKI (X.509) Certificate
  - Multiple Authentication
- End of Support for Vulnerable Algorithms/Protocols
  - MD5
  - SHA-1
  - BF-CBC
  - TLS 1.1
  - LOW security suite for TLS V1.2
- Compression Is No Longer Enabled by Default

*: Select SSL VPN to connect to a USG FLEX H series firewall.
*1: When connecting the SecuExtender IPSec/SSL VPN Client to a USG FLEX or ATP firewall, you can only use IPSec/IKEv2, because SSL VPN is not supported.

For more product information, visit us on the web at www.zyxel.com

25/09/23