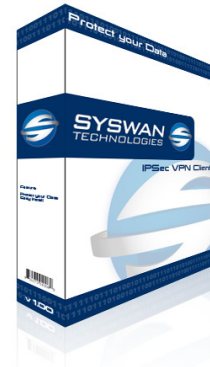


# Syswan VPN Client



## Overview

The Syswan VPN Client is a software implemented IPSec VPN solution that allows remote, mobile and home users to establish a secure and efficient connection to corporate networks over the Internet by creating point-to-point encrypted VPN tunnels. This on-demand IPSec VPN Client is compatible with all Syswan VPN load balancers and can also be interoperable with other IPSec VPN gateway products when needed to be used in a multi-vendor environment.

### Easy to configure and manage

Highly efficient and easy to configure, the Syswan VPN Client provides the most comprehensive interface on the market today. With its built-in configuration wizard and gateway configuration guides, administrators and end users can create VPN tunnel configurations easily.

### Maximum security

When connecting to a Syswan VPN load balancer, the Syswan VPN Client allows peers to authenticate using a preshared secret key. The Syswan VPN Client can also be configured to use certificates or username and password when connecting to other vendor VPN endpoints. The Syswan VPN Client runs on all current Microsoft operating systems and contains many security and control features such as Token Certificates Management, UBS token, Smartcard and secured import and export functions. It can also be used in a peer-to-peer environment.

### Reliable networking

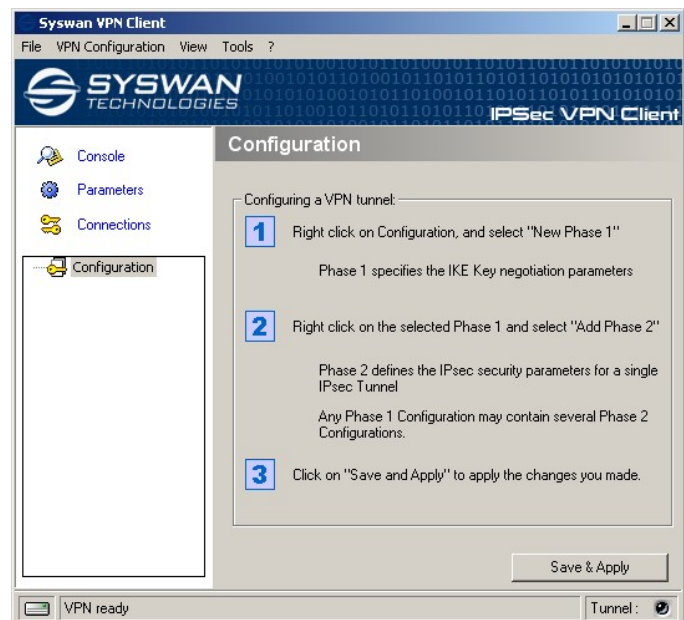
As more people rely on the Internet for communication, so too does the need to rely on scalable, secure and fast corporate connectivity. When integrating more business applications to your ever evolving network, it is extremely important that your organization's security is respected. This can be achieved by implementing the Syswan VPN gateway and client solution to always maintain absolute security.

Free 30 day trial version available.

## Key features :

- Compatible with all SYSWAN VPN load balancers
- Interoperability with other IPSec VPN Gateways
- IPSec VPN tunneling with DES / 3DES / AES encryption
- Internet Key Exchange (IKE) for user authentication
- Supports all connection type : DSL, dialup modem, Ethernet, wireless...
- DPD and Redundant gateways
- Mode-Config (auto, manual)
- Use USB Stick to store VPN Security Elements (network, key, certificates...)
- User Authentication with X-Auth, PEM or PKCS#12 Certificates, SmartCards, PreShared keys...
- Supports all current Microsoft Windows versions

### Software screen preview :



## Specifications

### Hash algorithms

- MD5-HMAC 128 bit authentication
- SHA1-HMAC 160-bit authentication

### Encryption

- DES-CBC 56 bit encryption
- 3DES-CBC 168 bit encryption
- AES 128, 192, 256 bit encryption

### Diffie Hellman Group Support

- Group 1 : MODP 768
- Group 2 : MODP 1024
- Group 5 : MODP 1536
- Group 14 : MODP 2048

### Authentication Mechanism

- Pre shared Key
- X509 Certificate support
- X-Auth
- SmartCard & Token (Aladdin, ..)

### Certificate

- Flexible Certificate Support (PEM, PKCS#12, ...)

### Key Management

- ISAKMP (RFC2408)
- IKE (RFC2409)

### IKE & IPsec Mode

- ESP, Tunnel, Transport
- Main, Aggressive, Quick
- Hybrid Authentication Method

### USB stick mode

- All formats supported (SD, MMC...)
- Auto close, Auto open IPsec tunnels when plug in or remove USB Stick
- Security Elements (e.g. network configuration, shared key, certificates...) cannot be used on other computers

### Networking

- NAT traversal (Draft1, 2 & 3) allows IPsec connection through a NAT device
- Main mode & aggressive mode
- NAT keep Alive, Payload NAT\_OA, IP address emulation
- Forced NAT-T
- Multi tunneling to several Gateways
- Dead Peer Detection (DPD) support

### Connection Technologies

- DSL, dial-up modem, GPRS-Edge-3G, Ethernet, PCMCIA cards, WIFI ...

### Redundant Gateway

- Redundant gateway when primary is down or not responding
- Use of DPD (Dead Peer Detection) for fail over

### Config-Mode

- Automatically fetch remote network DNS and WINS server addresses
- Manual Config-Mode in case remote gateway doesn't support Config-Mode

### Peer to Peer

- Peer to Peer connections
- Accepts incoming IPsec Tunnels

### Blocking capabilities

- IPsec only traffic filtering
- Can block all other connections than the VPN connections

### Management Options

- Access control to Configuration Panel
- Can run fully invisible to users (hidden mode)
- Set of command lines to make easier deployment and management
- Capability to start before logon
- Launch script when tunnel open

### Phase 1 and phase 2 configuration screen preview :

