

Propalms



VPN

Access Made Easy

Propalms VPN is an easy-to-use, simple to integrate, application access and security product for enabling high-trust, secure remote access to corporate applications and resources. Enterprises use Propalms VPN to collaborate securely with employees, customers and partners.

It enables secure access to all applications for all users in a scalable, highly performing manner that works for distributed offices, mobile users and wireless LANs. Users establish secured sessions simply by clicking on a URL on the VPN gateway login page. Upon successful authentication, the client computer receives configuration details from the VPN gateway and policy controlled access to the Private network.

All application traffic is managed by the Propalms VPN Server, simplifying firewall administration. Network administrators no longer have to create and manage firewall rules for individual users to access specific external applications. As part of an integrated policy infrastructure, it ensures that users can only access authorized resources. Since application connectivity is managed centrally, operational costs are reduced and overall network security is improved.



KEY FEATURES:

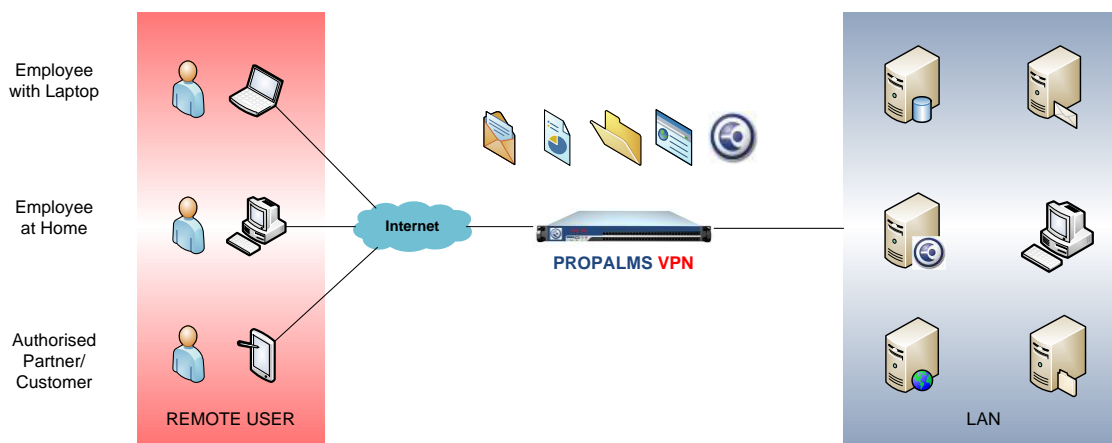
- **Application Support** allows access to virtually any application, including all TCP, 802.11x and UDP applications, Microsoft Outlook, FTP, Propalms TSE, Microsoft Terminal servers. Even custom or proprietary applications and protocols are supported by the Propalms SSL VPN.
- **Secure Firewall Traversal of TCP/UDP** allows local desktops to access UDP-based remote data services, without segregating the network, exposing UDP port ranges to hackers, using routable IP addresses, or publishing internal routes externally. Propalms VPN works alongside existing firewalls, and NAT devices.
- **Authentication and authorization architecture** supports different group access policies via leading protocols (LDAP, Active Directory, RADIUS, and more).
- **Centralized Access Control** manages granular access control by source, destination, domain name, user group, port, host, or network thereby, increasing security and dramatically simplifying firewall configuration.
- **Single Mode Connectivity** enables remote access to any application, including web-enabled and legacy applications, through a simple interface with the look and feel of the user's native desktop.
- **Load Balancing and High Availability** automatically distributes application network traffic among multiple VPN Servers with integrated failover to available servers.
- **SSL VPN** users may access applications from a standard portal interface or directly from their desktop, for an IPSec-like "in office" experience.
- **Clientless browser-based access** provides secure remote access to applications through common web browsers. No clients to install or maintain.
- **Split Tunneling** enables accessing of resources from multiple networks simultaneously.

BENEFITS

- **Reduced Costs** - centralize management; consolidate data centers, lower administration costs.
- **Investment Protection** - utilize existing networks, firewalls, servers, clients and software.
- **Trusted Remote Access** - extend access to regional offices, partners, customers, telecommuters, wireless users.
- **Easy to Use** - fast installation and little ongoing management, reduced training, less down-time.
- **Continuous Access** - provide reliable, available and scalable access.
- **Printing** - printing from centralized applications to local printers for remote users.

ACCESS

- **Email Access** - Use your local Outlook or Lotus Notes client to access corporate email system.
- **File Shares and FTP** - directly access the files and shares residing on the corporate network.
- **Web Applications** – access any http/s based applications.
- **Propalms TSE and Terminal Services** – secure connection to RDP based applications
- **Legacy Applications** – provide access to any TCP/UDP based applications.



DETAILS

<p>Performance and Reliability</p> <ul style="list-style-type: none"> · High Availability, Load Balancing 	<p>Access Control Criteria</p> <ul style="list-style-type: none"> · IP Address (Source and Destination) · Group, Time 	<p>Key Exchange:</p> <ul style="list-style-type: none"> · RSA · Diffie Hellman 	<p>Hardware</p> <ul style="list-style-type: none"> · Intel P 4 2.5GHz, 512MB RAM, 40GB Hard Disk · Appliance Model includes hardened, high-performance OS.
<p>Administration Tools</p> <ul style="list-style-type: none"> · Web-based Management Console · Real-time status and monitoring · Role-based administration. · Time based access · Groups and Policies 	<p>Connectivity and NAT</p> <ul style="list-style-type: none"> · Co works with Network Address Translation (NAT) and Firewall · VPN Chaining 	<p>Certification Authority</p> <ul style="list-style-type: none"> · Enterprise PKI Built In with X509 Standards 	<p>Clientless Agent OS (ActiveX required on all)</p> <ul style="list-style-type: none"> · Microsoft Windows Xp® (Sp2) · Microsoft Windows 2003® · Microsoft Windows
<p>Auditing and Logging</p> <ul style="list-style-type: none"> · Session, connection, failed connection · logging; Administrative Auditing 	<p>Encryption Standards</p> <ul style="list-style-type: none"> · RC4 with 128-bits · 3DES · AES with 256-bits · SHA Hash · Md5 Hash 	<p>Authentication Mechanisms</p> <ul style="list-style-type: none"> · Active Directory Services; · LDAP; · RADIUS · RSA SecurID® · X.509 Digital Certificates · Finger Print Biometrics 	