



## SECURE REMOTE ACCESS FOR THE ENTERPRISE

Propalms VPN is an easy-to-use, simple application access and security solution (SSL VPN) for enabling high-trust, secure remote access to corporate applications and resources.

### SECURE APPLICATION GATEWAY

Today, organizations of all sizes face the pressure to be able to deliver applications and data to ever increasing numbers of mobile workers. Whether this is home users, roaming users, customers or even business partners the need for a Secure Remote Access solution that is easy to use and yet secure is the key requirement; this is where Propalms VPN can help.

When implementing a VPN it is important for organizations to consider the VPN technology. Current VPNs whether IPSec or SSL VPNs rely on layer 2 VPNs to provide seamless access to applications. This creates a security hole in perimeter security deployed at the corporate network level and opens up the network to unknown vulnerabilities generated from unmanaged desktop machines. It should be noted that the requirement is to deliver the application and network services to end-users rather than necessarily bridging unknown endpoints to corporate networks at untrusted locations.

Propalms VPN is an application gateway that provides secure access to the applications using standards based SSL encryption. Propalms VPN enables access to specified applications only, rather than bridging end-user's machines with the corporate network, while still maintaining full application compatibility. Propalms VPN comes with unique network obfuscation feature which hides the internal network details from intentional or unintentional exploitation by a user or hacker.

Propalms VPN brings together the performance, management and functionality required for enterprise remote access and reduces costs traditionally associated with other VPN solutions due to the simplicity and ease of use of our solution united with our low license costs.

### ENDPOINT SECURITY (DEVICE PROFILING)

The primary driving factor for wide adoption of SSL VPNs is ubiquitous secure access from any device without any pre-requisites. However this opens up a new challenge for organizations as unknown and unmanaged devices including potentially harmful devices can connect to the corporate network. Moreover compliance becomes a challenge as it becomes impossible to enforce corporate policies to end users. Next generation SSL VPNs like Propalms VPN bring strong device profiling features that measure and calibrate each endpoint connecting to VPN against the corporate policies. Propalms VPN provides a flexible policy framework for administrators to keep the corporate network safe from unclean devices by either keeping such devices out of network, restricting them to a part of network or remediate them to be able to access network services.

As part of device profiling, Propalms VPN can check for status of endpoint security software like antivirus, firewall and anti-spyware, OS and software updates and compliance to endpoint configurations. An intelligent cache wiper can clean the files and cache stored on the local hard disk by browsers or by users, whether residing in temporary folders or any of the drives. To protect zero day attacks the Meta data about the latest virus signatures is pushed to Propalms VPN gateway every hour.

### DYNAMIC GRANULAR POLICY CONTROL

An organization can have different types of users based on their location and their role. These may be trusted employees working from trusted or untrusted networks or they might be known partners, consultants who need access to applications from their respective location. There could even be users who are completely unknown to organizations who can request application access from any network. These users may use trusted or untrusted devices and may be working from similar trusted or untrusted networks. For each such user case, enterprises must protect the applications and network against unauthorized access and intentional or unintentional information leakage. The remote access solution employed by the organization must provide a flexible and dynamic policy framework which can adjust on run time to accommodate users coming from different locations or devices but at the same time protect the applications in case the point of access becomes in-compliant to corporate security needs.

Propalms VPN has a dynamic multi-layered policy engine that evaluates the user session at multiple levels before access to an application is granted. Before access to an application is granted each session is evaluated against policies set for the location of the user, method of authentication chosen by user, trust level of the endpoint device and finally the role of the user. The evaluation is done on the fly and an application is restricted as per any of the failed criteria and hidden from the user.

## Protect

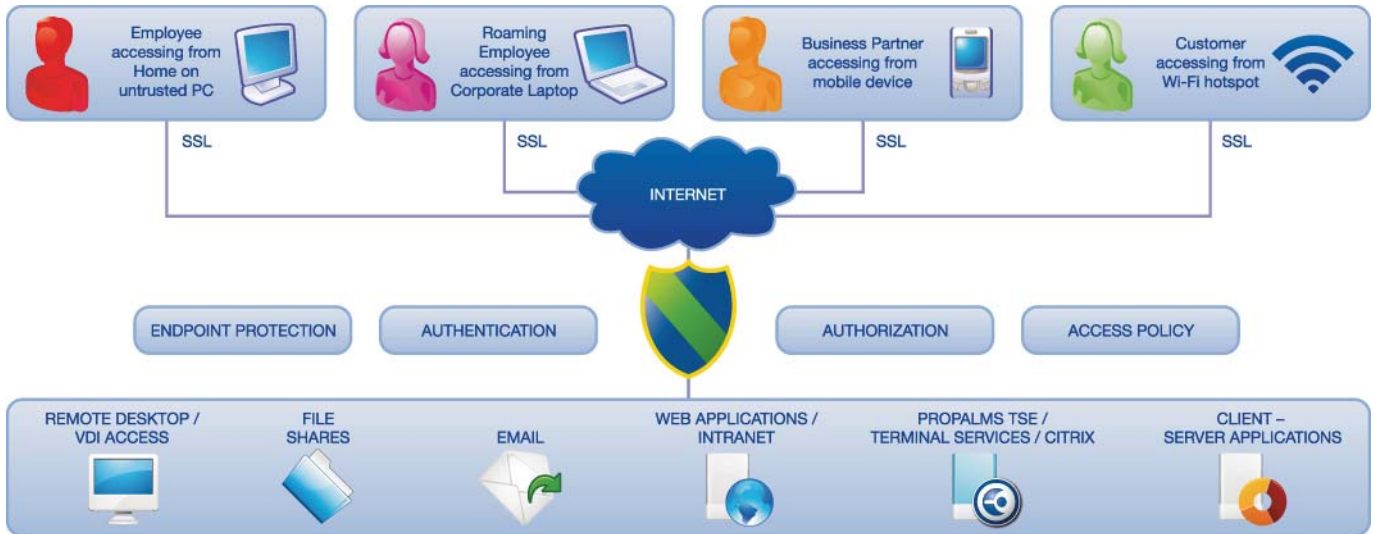


## Secure



## Deliver





### SPAN TECHNOLOGY

Propalms SPAN (Secure Private Appliance Network) technology enables a completely secure access method over any kind of network and devices. With SPAN technology, Propalms VPN can make applications available without bridging client device's network with the corporate network. Other VPN solutions require a network adaptor with virtual IP Address for full functioning of client-server applications. SPAN technology has following salient features:

- Secure remote access without creating unsecured holes in the network's perimeter security.
- Makes application access possible without a virtual adaptor or routing changes on endpoint machine.
- Hide complete network information obfuscation. User can never find the actual IP address of hostname of the internal servers.
- Administrator can control each application available over VPN rather than opening up the whole network/subnets.

### ACCESS YOUR APPLICATIONS

Access all of your Applications, including all TCP, 802.11x and UDP applications, Microsoft Outlook, FTP, Propalms TSE, and Microsoft Terminal Servers. Even custom or proprietary applications and protocols are supported by the Propalms VPN.

### ENDPOINT SECURITY

Enforces access restrictions based on customizable policies such as Anti-virus, Anti-spyware and firewall status ensuring devices are 'safe' for connection to the network. Real time, hourly updates for over 200 products ensures protection against any zero day attacks.

### SECURE AUTHENTICATION

Propalms VPN uses standards-based SSL/TLS Security. Users can be authenticated by methods such as Active Directory, LDAP, and RADIUS. Fully integrated client-certificate based two factor authentication with automatic certificate provisioning is built in to the VPN. Configurable Authentication and Authorization servers mean that users can login using multiple methods and still have resources assigned by Group or Role.

### GRANULAR ACCESS CONTROL

Administrators can create policy based access control for restricting users to specific applications and resources and preventing unauthorized access. Access control based on Device identity and profile, User Authentication method and User Role with Time-based restriction policies for further lockdown capabilities.

### INTEGRATED FULLY AUTOMATIC CA

Propalms VPN has a fully integrated CA function that makes certificate creation, provisioning, enrollment and revocation completely automated and easy to manage. Other SSL VPNs do provide certificate based authentication but none of them provides client certificate provisioning and management. Also Propalms certificate distribution and enrollment is completely secure as the user's password and certificate are never transmitted over the wire. Even the VPN administrator cannot login as some other user in the system.

### SITE TO SITE ACCESS

Propalms VPN provides a unique Site-to-Site access feature where it is possible to chain the Propalms VPN gateway and access applications across sites. Other VPNs either provide IPSec based site to site or their SSL based Site-to-Site is layer 2 tunnel which suffer from poor performance because of too much packet loss. (Read 'TCP-over-TCP meltdown').

### EASY MANAGEMENT

Web based Management Interface with real-time dashboard updates and in-line help make administration simple. Delegated administration and secure, certificate based login for Administrators ensures that the VPN is protected against unauthorized admin access.

### DEPLOYMENT

Install in minutes using a simple, integrated installer or save even more time by downloading the Propalms VPN Virtual Appliance and import it directly into your VMware infrastructure or your other chosen virtualization platforms.

### HIGH AVAILABILITY & PERFORMANCE

Scalable to 200,000 users with built-in Load Balancing, Propalms VPN automatically can distribute application network traffic among multiple VPN Servers with integrated failover to available servers. Propalms VPN has been built for thousands of users and has been tested in a live environment with 30,000 users.

### CLIENT ACCESS

Web Portal provides easy access for end users and Clientless VPN agent for seamless access to applications.

### INTEGRATION WITH PROPALMS TSE

Propalms VPN works in conjunction with Propalms TSE solution to deliver a highly efficient application delivery solution to enterprises. Propalms TSE provides presentation virtualization and VPN provides remote access. Propalms VPN enables Single Sign ON and auto-launch features for Propalms TSE enabled applications.



## Web Based Management

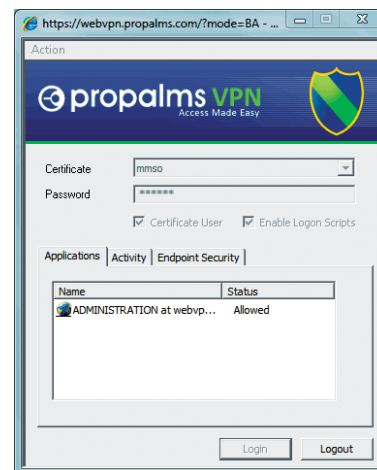
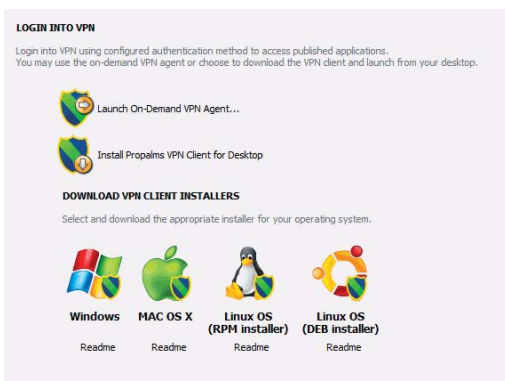
The Propalms VPN solution has an intuitive, easy to use web interface with graphical dashboard allowing administrators to deploy, configure and monitor the VPN server from any web browser. Administrators can login using high-security, certificate based authentication providing an extra level of security.

Administrators can perform tasks such as:

- Create/Add Users (native, LDAP, Active Directory)
- Create User and Application Groups for defining access to applications.
- Control device access using Endpoint Policies and Zones.
- Specify time-based access restrictions.
- View Reports and manage current sessions.
- And more...

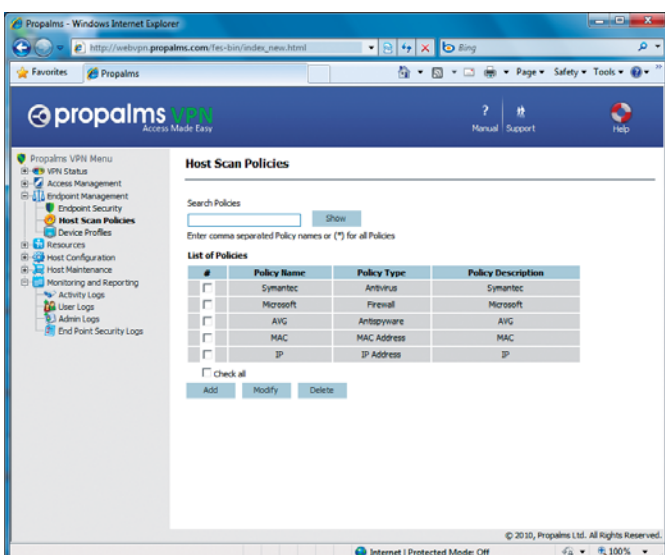
## On-Demand VPN Agent...

For Clientless access, you can use your browser and launch the Propalms 'On-Demand VPN Agent' from the VPN landing page. Users simply click the link and login using their username and password to get access to their authorized applications and resources. This client provides connectivity without a user having to install any local application helping reduce complexity and management costs.



## ...and Desktop Clients

Propalms VPN has client support for Windows, Mac OS and Linux. Simply login to the VPN portal Website and click on the client that you require and installation will happen instantly.



## Endpoint Management

Although SSL VPNs provide broader access capability which clearly enhances productivity, it also inherently widens network exposure to uncontrolled environments. For Example: If a remote client machine is infected with virus/worms/Trojans/spy-wares, this un-wanted traffic is also sent to private network over secured connection. To effectively control these risks, it is no longer enough to manage access by user identity alone. The safety of the user's end point environment must also be ensured by enforcing access policies based upon solid end point protection.

Propalms VPN Administrators can create three types of product policies; Antivirus, Antispyware and Firewall ensuring the most recent versions are installed and active on the user's device before they can connect to the network. Further to this, Administrator's can create Endpoint Zones which override Application Groups limiting access to applications based on the result of the user's device profile from the Endpoint scan. For example, a 'Quarantine' Zone can be set to provide minimal access for non-compliant devices connecting to the VPN.



<p><b>DEPLOYMENT SCALABILITY</b></p> <ul style="list-style-type: none"> <li>- Scalable to 200,000 users</li> <li>- Active-Active N+1 cluster</li> <li>- Resource based VPN Load balancing with multiple load balancer</li> <li>- Session Persistence: Users do not need to re-authenticate</li> </ul>	<p><b>APPLICATION SUPPORT</b></p> <ul style="list-style-type: none"> <li>- All web based, TCP and UDP based client-server applications</li> <li>- Windows File Shares and Drive Mapping</li> <li>- Dynamic port based applications</li> <li>- Special support for RDP virtual channels</li> <li>- Application load balancing</li> <li>- Session Caching for load balanced applications</li> <li>- Per application based compression switch</li> </ul>	<p><b>ACCESS SECURITY FEATURES</b></p> <ul style="list-style-type: none"> <li>- SSL 3.0 and TLS 1.0</li> <li>- Encryption: Strongest available: DES, 3DES, AES(256), RC4</li> <li>- Authentication: MD-5, SHA-1, RSA 1024, RSA 2048</li> <li>- Internet network masking and IP address/hostname mangling</li> <li>- Application level gateway and not layer 2 bridging</li> <li>- Hardened Gateway Operating System</li> </ul>
<p><b>AUTHENTICATION FEATURES</b></p> <ul style="list-style-type: none"> <li>- Authentication based on user identity, endpoint identity, endpoint trust level</li> <li>- Multiple User authentication options: static passwords, client certificates, External two factor authentication solutions</li> <li>- Local database with full customization per user, password policies, password reset support</li> <li>- Fully integrated client-certificate based two factor authentication server with automatic CA and certificate provisioning</li> <li>- Email based user provisioning</li> <li>- Authentication method based application access control</li> <li>- Integrates with AD/LDAP/RADIUS</li> <li>- Automatic fetching of group information from AD/LDAP/RADIUS</li> <li>- Support for multiple Authentication Servers with cascading mode</li> <li>- Support for External Authorization Servers</li> </ul>	<p><b>AUTHORIZATION FEATURES</b></p> <ul style="list-style-type: none"> <li>- Publish applications rather than subnet or network</li> <li>- Simple access control mechanism</li> <li>- Access control based on             <ul style="list-style-type: none"> <li>· Device identity and profile</li> <li>· User Authentication method</li> <li>· User Role</li> </ul> </li> <li>- Dynamic policy evaluation based on run time information about device, authentication method and user role</li> <li>- Display of allowed applications and availability of the application server to users</li> <li>- Time based restriction policies</li> <li>- Auto-detection of applications running in corporate network</li> <li>- Scheduled account expiry</li> <li>- Block specific groups</li> </ul>	<p><b>AUDITING FEATURES</b></p> <ul style="list-style-type: none"> <li>- Complete reporting of user logons and activity</li> <li>- Information logged includes             <ul style="list-style-type: none"> <li>· Time of access</li> <li>· Username</li> <li>· MAC Address of endpoint</li> <li>· IP address of endpoint</li> <li>· Application accessed</li> <li>· Device Profile</li> </ul> </li> <li>- Logging of endpoint security scans</li> <li>- Detailed logging per device scans including             <ul style="list-style-type: none"> <li>· Policies evaluated for user sessions</li> <li>· Current profile of endpoint</li> <li>· List of failed policies</li> <li>· List of policies for which remediation information is sent to user</li> </ul> </li> <li>- Extract logs in CSV format for feeding to third part report generation</li> <li>- Auto-archiving of logs</li> <li>- Monitor and disconnect live users</li> </ul>
<p><b>ENDPOINT MANAGEMENT</b></p> <ul style="list-style-type: none"> <li>- Support for checking for Antivirus, Firewall and Antispyware products</li> <li>- Real time status check for             <ul style="list-style-type: none"> <li>· Virus signature DAT file version</li> <li>· Last update time</li> <li>· Last scan time</li> <li>· Real time protection check</li> </ul> </li> <li>- Support for more than 1100 products</li> <li>- Support for checking for MAC ID and IP address</li> <li>- Application control based on device profile</li> <li>- Mandatory profile for non-avoidable policy checks on all endpoints</li> <li>- Quarantine profile for devices that fails all other profile</li> <li>- Option to block endpoints that fails to comply to required policies or option to allow them to login by putting them in quarantine profile</li> <li>- Real time updates about latest virus signature DAT file releases by AV/FW vendors are pushed to VPN gateway every hour to protect corporate network against any zero day attacks</li> <li>- Integrated with OPSWAT™ endpoint security SDK</li> <li>- Automatic remediation of endpoints</li> </ul>	<p><b>ACCESS MODES</b></p> <ul style="list-style-type: none"> <li>- Web Portal for easy access by end users</li> <li>- Clientless VPN with a browser agent for seamless access to applications</li> <li>- No configuration required on end user machines</li> <li>- Client platforms supported             <ul style="list-style-type: none"> <li>· Windows 98/XP/Vista/Windows7</li> <li>· Windows server 2003/2008</li> <li>· Linux OS</li> <li>· MAC OS X PPC/Intel 10.4 and above</li> </ul> </li> <li>- Site to Site access</li> </ul>	<p><b>MANAGEMENT</b></p> <ul style="list-style-type: none"> <li>- Web based management console</li> <li>- Dashboard with graphical reporting</li> <li>- Menu driven console interface for system configuration</li> <li>- Wizard driven installation procedure</li> <li>- Self signed certificate generation</li> <li>- CLI</li> <li>- Delegated administration</li> <li>- Certificate based strong authentication for administrators</li> <li>- Auto checking for configuration errors</li> </ul>
	<p><b>GATEWAY FEATURES</b></p> <ul style="list-style-type: none"> <li>- Runs on hardened Linux based platform</li> <li>- Menu driven console interface for easy configuration</li> <li>- Can run on any standard or custom hardware</li> <li>- Runs on Virtualization platforms, VMware, XenServer, Hyper-V</li> </ul>	<p><b>COMING SOON...</b></p> <ul style="list-style-type: none"> <li>- Kiosk based application portal</li> <li>- Layer 2 VPN mode</li> <li>- Integrated 2 factor authentication feature for OTP and SMS based authentication</li> <li>- Endpoint security for Linux and MAC OS X</li> <li>- VPN client for WinCE and iPhone</li> </ul>



**EMEA / APAC**  
 Email: sales@propalms.com  
 Tel: +44 (0)1653 696060  
 Fax: +44 (0)1653 693040

**USA**  
 Email: sales@propalms.com  
 Tel: +1 407 571 6827  
 Fax: +1 407 571 6801

**INDIA**  
 Email: indiasales@propalms.com  
 Tel: +91 22 4090 7360  
 Fax: +91 22 4090 7340



**For more information go to <http://www.propalms.com>**