



Secure Resilient Networks

Secure remote access

Enabling your workforce to work quickly and securely

One of the most important requirements for almost all of our customers is the ability for their employees to be able to safely access the corporate IT systems and data - no matter where they are. CI-Net helps ensure that information in your business flows freely but securely by delivering tailored VPN solutions that meet your individual needs.

VPN solutions enable your entire workforce, whether they are working at a remote office, from home, a hotel or airport lounge, to interact quickly and securely. A well-executed VPN solution is built around existing Internet infrastructures, and should offer familiarity and compatibility with the in-office experience. VPNs might offer an incredibly cost-effective solution, but getting it right for everyone is essential.

VPN for your worldwide locations

IPSec VPN enables fast, economical, secure and fully meshed communications between your remote offices. CI-Net can rapidly configure and deploy a system so that all your remote locations can safely communicate with each other directly, which means an outage at head office will not affect the whole VPN. Our central management centre can also handle the ongoing management.

At CI-Net we spend time finding out about how your business operates so that we can recommend the best tools to enable your entire workforce to communicate.

VPN access from any Internet enabled PC

Making business applications remotely available to home workers and travelling staff is vital for most companies. With CI-Net's SSL VPN, remote users can quickly and securely reach the resources they need. An integrated radius server for two factor authentication and Federal Information Processing Standards mean our VPN meets the most stringent security standards.

iPass Global Roaming

iPass gives your mobile workforce around the world a safe, simple, low-cost way to connect to your systems from non-company locations such as hotels or Wi-Fi hotspots. With the worlds largest virtual network your users can dial up from 160 countries and over 78,000 hotspots.

Security Assured

CI-Net can provide a VASCO security device giving two factor user authentication for any radius environment so you can be sure who is accessing your systems.

By installing our secure firewalls and intrusion protection system based on StoneGate technology you can proactively defend your corporate network by detecting and blocking malicious packets in regular network traffic before any damage occurs.



Please contact us for further information

CI-Net Network House Langford Locks Kidlington Oxfordshire OX5 1GA

TELEPHONE 01865 856000 FAX 01865 856001 EMAIL info@ci-net.com WEB www.ci-net.com

IPSec VPN

Ideal for fixed locations such as regional or worldwide offices. A CI-Net IPSec VPN enables fast, economical, secure and fully meshed communications between your offices. In addition CI-Net can fully manage your IPSec VPN using our management centre for ease of configuring, deploying and on-going support.

Security: In an IPSec VPN all devices communicating with each other must use a common key and the firewalls of each network must have very similar security policies in place. Deploying and managing this can be a very time consuming task. CI-Net can rapidly configure and deploy your IPSec VPN from a central management centre eliminating the costly process of your IT department having to visit each site. This also dramatically simplifies the ongoing support and maintenance. For additional security CI-Net can encrypt data between devices.

Resiliency: Using a standard CI-Net VPN, based on StoneGates, the VPN can be fully meshed so that each remote site can communicate with all other sites directly. Thus if there is an outage at head-office it does not adversely affect the whole VPN.

Flexibility & Managed Services: One of the issues that many companies wrestle with when deploying IPSec VPNs is the set-up and ongoing management of the routers and firewalls, especially at remote sites. CI-Net uses a centralised management centre and offers fully managed services to eliminate this time consuming and complex process.

Secure SSL VPN

Ideal for home workers and travelling workers in un-trusted environment such as hotel and airport Internet kiosks. Secure Socket Layer (SSL) needs no software or configuration on the client device and can easily be combined with two factor authentication. Secure reliable access from any PC with Internet Explorer or Firefox, anywhere in the world.

Security: CI-Net has standardised on the AEP Netilla platform for SSL VPNs. Netilla Security Platform SSL VPN (NSP) helps companies satisfy one of their most pressing needs: making business applications remotely available to employees and partners. With the NSP, remote users can quickly and securely reach the varied resources found in today's IT environment, including Microsoft Outlook, Windows Terminal Servers and

server-based applications, as well as client/server applications over an SSL tunnel.

NSP with Federal Information Processing Standards (FIPS) support is designed to provide secure remote access to highly confidential data to meet the most stringent U.S., Canadian and U.K. security standards.

Flexibility: The NSP is available in several classes designed to meet your organisation's capacity needs. It is a feature rich platform:-

- Easy to use, Web-based access to Citrix, Windows, X11, UNIX, and Linux Terminal Servers, and Mainframe (3270/5250)
- Policy-enforced deployment of individual applications through an icon-driven webtop
- Policy-enforced Web application access via secure web reverse proxy and unique Java rewrite technology
- Sophisticated V-Realms authentication and authorisation architecture integrates seamlessly with existing authentication infrastructures (LDAP/AD/Radius/PKI/2-Factor/NT Domain)
- Policy-enforced network extension capabilities for VOIP and other TCP or UDP based applications
- Client integrity tools eliminate data theft (cache cleaning, secure desktop, host integrity, adaptive policies, machine identification)
- Web application security protects against cookie snooping, denial of service and network access attacks, authentication hijacking, DMZ protocol attacks, man in the middle attacks, and more.
- Powerful, VPNC and ICSA Labs-approved security at the network edge
- Surprisingly quick installation and little ongoing management
- High productivity: print, move files, leverage high-colour applications (like CAD/CAM, X-Ray and imaging) and work anywhere.

Managed Services: CI-Net professional services are adept at implementing and supporting SSL VPNs for our customers.

Please contact us for further information

CI-Net Network House Langford Locks Kidlington Oxfordshire OX5 1GA

TELEPHONE 01865 856000 FAX 01865 856001 EMAIL info@ci-net.com WEB www.ci-net.com