

Secure VPN Solution

The easiest way to deploy, administer and grow your secure Virtual Private Network

Introduction

VPNs offer organizations a cost effective and secure method of providing access to internal networks using public networks such as the Internet. VPN technology provides network level security for telecommuters, site-to-site communication for branch and corporate offices (intranets) and business-to-business communication for companies to securely communicate with their business partners (extranets).

The accepted standard for Internet-based VPNs is the Internet Protocol Security (IPSec) protocol as specified by the Internet Engineering Task Force (IETF). Authentication in IPSec can be provided through the use of Digital Certificates or shared secrets.

Baltimore's Secure VPN Solution supports the deployment of IPSec Digital Certificates for several industry-leading VPN products. Securing your IPSec VPN with Digital Certificates provides a cost-effective, easy to use and highly scalable method for remote users to access to your internal network.

Shared Secrets vs. Digital Certificates

Using shared secrets as a method of authentication is practical only in small VPN deployments and where communication is limited to within the enterprise. Maintaining shared secrets for more than a few VPN devices becomes increasingly difficult to manage since shared secrets are typically distributed manually, can be compromised, and require significant help-desk support.

Digital Certificates make scaling secure VPNs much easier. Adding users to your Secure Virtual Private Network is easy. New users simply need to obtain a Digital Certificate issued by a Certificate Authority. The CA issues certificates based on your organization's approval instructions, keeping you in control of the issuance and revocation of Digital Certificates to end users within your VPN. Deleting users is just as fast and easy with the incorporation of Certificate Revocation Lists (CRLs) into your secure VPN solution.

Supplying the Solution

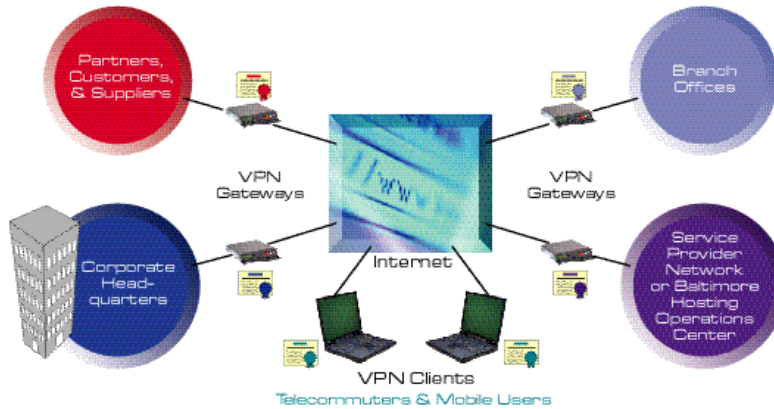
By implementing Baltimore's Secure VPN, organizations can solve communication problems while enjoying significant cost savings. Baltimore takes three essential components:

- **UniCERT CA**
- **LDAP Directory**
- **Customer-furnished VPN devices**

and combines them with comprehensive training and documentation, resulting in an easy to use and manage VPN solution that is deployed in a fraction of the time otherwise needed.

All Baltimore SolutionsPlus feature UniCERT OptionsTM. Based on award-winning UniCERTTM technology, UniCERT Options is a complete set of PKI offerings ranging from out-sourced CA hosting to in-house CA product deployment options, consulting services and extended Public Key Infrastructure components.

Features	Benefits
IPSec compliant X.509 Digital Certificates and full standards-based solution	Strong Authentication - Digital Certificates provide the strongest level of authentication a corporation can use to enable trust between relying parties.
Remote Registration Authority	Remote Registration Authority features allow unlimited administrators the ability to concurrently perform RA duties from dispersed geographic locations.
Ease of use for end users	VPN end-users will transparently use Digital Certificates to securely connect to internal networks
Easy for IT to administer	IT will enjoy the simplicity of deploying a VPN with Digital Certificates as well as the reduced on-going burden that comes with eliminating password and shared secrets.
Interoperability with leading VPN vendors	Baltimore VPN solutions have been fully tested and integrated with leading VPN devices as well as LDAP-compliant X.500 directories for CRL support.

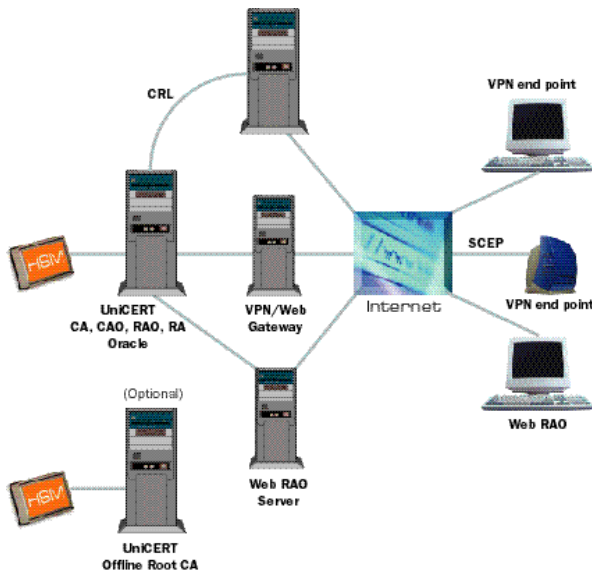


Baltimore's Secure VPN Solution provides the most secure and easily administered method for deploying certificate-enabled VPNs

Secure VPN Solution Configurations Available	
CA Configuration Options	<ul style="list-style-type: none"> In-sourced Product Hosted Service
Operating Systems	<ul style="list-style-type: none"> Windows NT UNIX
Packages Available	<ul style="list-style-type: none"> Enterprise Customers Service Providers (ISPs, ASPs)

Secure VPN Solution Components	
UniCERT OptionsTM	The UniCERT Certification Authority is designed to implement flexible security solutions and complement the way your organization does business. UniCERT architecture easily evolves to meet your changing requirements such as the integration of new applications, additional users, interoperability with partner organizations and changes in your organization's infrastructure.
VPN Device: Gateway and Client (Customer Furnished)	Fully Integrated VPN solutions with the leading VPN suppliers: <ul style="list-style-type: none"> Cisco - 3640 Router and Client Cisco VPN 3000 Concentrator v2.1 Alcatel - Timestep Permit Gate/Client - (currently only available as hosted option) Check Point Software Technologies FW-1 and SecuRemote version 4.1 Nortel Contivity Switch and Client - (coming soon)
LDAP-compliant Directory	Posting CRLs to an X.500 directory provides an efficient method to deal with constantly changing user group. Note: Baltimore's VPN Solution utilizes the Netscape Directory Server 4.0
Training	In-depth training for both product and hosted deployments
Documentation	Specialized documentation that provides step-by-step instructions according to VPN device selection provided
Technical Support	7 X 24 support available for both product and hosting options
Professional Services (if required)	Experts to help design and implement the secure VPN infrastructure of choice

Secure VPN Solution Architecture



The Secure VPN Solution architecture is standards compliant, supports leading vendor enrollment processes and is equipped to handle multiple authorization methods providing exceptional scalability.

www.baltimore.com info@baltimore.com