msctrustgate.com

Go Secure!
for Virtual Private Networks

Go Secure! for Virtual Private Networks (VPNs) ensures the confidentiality and integrity of your VPN and authenticates the identities of its users by issuing IPSec digital certificates to every client and device (including firewalls, routers, and servers) on your VPN, without proprietary hardware and software or time-consuming training and maintenance.

VPN Security

Enterprise across the world are opening up their corporate networks to remote employees, branch offices, business partners and customers by implementing Virtual Private Networks (VPNs) – a transparent, secure, and private connection across the Internet. With VPN, an authorized user in a remote location can simply dial in to local ISP and initiate a connection back to his or her network. VPN's benefits include: mobility, cost saving, streamlined business processes, improve communication, and improve customer satisfaction.

In order to achieve a secure, scalable and manageable VPN, network administrators require a quick and easy-to-deploy secure network infrastructure based on digital certificate services. Go Secure! for Checkpoint and Go Secure! for Nortel provide a fully managed digital service to speed the deployment of these VPNs. The digital certificates act as electronic credentials to authenticate remote sites, employees, business partners and customers, thereby ensuring that only the intended recipients or network devices have access to transmitted information.

Features and Benefits:

- Ease of Use
  Go Secure! for Checkpoint and Go Secure! for Nortel make it easier for end-users to secure their communications and transactions through automated lifecycle services for certificate acquisition, use, replacement and renewal.

- Compatibility with Leading Vendors
  Many vendors have implemented certificate lifecycle management components into their VPN gateways, firewalls, routers and desktop clients by employing industry standard protocols. This allows them to work seamlessly with Managed PKI without having to incorporate and support proprietary, single vendor oriented components into their products. The quick time-to-deployment and secure, highly available infrastructure of Managed PKI can be leveraged by vendors using SCEP, PKCS12, PKCS10, PKCS7, CRS, CSR, CMC, CAPI and others.

- Integration with Multi-factor Authentication Devices
  To ensure the highest level of security, many enterprises provide their end-users with authentication devices such as smart cards and USB tokens. When used in conjunction with digital certificates, this provides an unparalleled level of security for remote users who log in through VPNs.

- Network Administrator Benefits
  Go Secure! for Checkpoint and Go Secure! for Nortel solutions free network administrators from the time-consuming burden of manually generating, distributing, renewing, and publishing digital certificates, and certificate revocation lists (CRLs). These VPN remote access clients can automatically request and receive certificate management services from MSC Trustgate. Automated approval of certificate requests without local programming or database management saves the customer time and manpower.

MSC Trustgate.com Sdn Bhd (478231-X)
CA License No. LK 0022000
Ground Floor, Belatuk Block, Cyberview Garden, 63000 Cyberjaya, Selangor, Malaysia
Telephone: +6 (03) 8318 1800 Facsimile: +6 (03) 8319 1800 E-mail: sales@msctrustgate.com
Web site: www.msctrustgate.com

VeriSign TRUST NETWORK