V-ONE
Security for a Connected World

SmartGate

Addressing the Opportunity of Virtual Private Networking

David Hawkins

August 1998

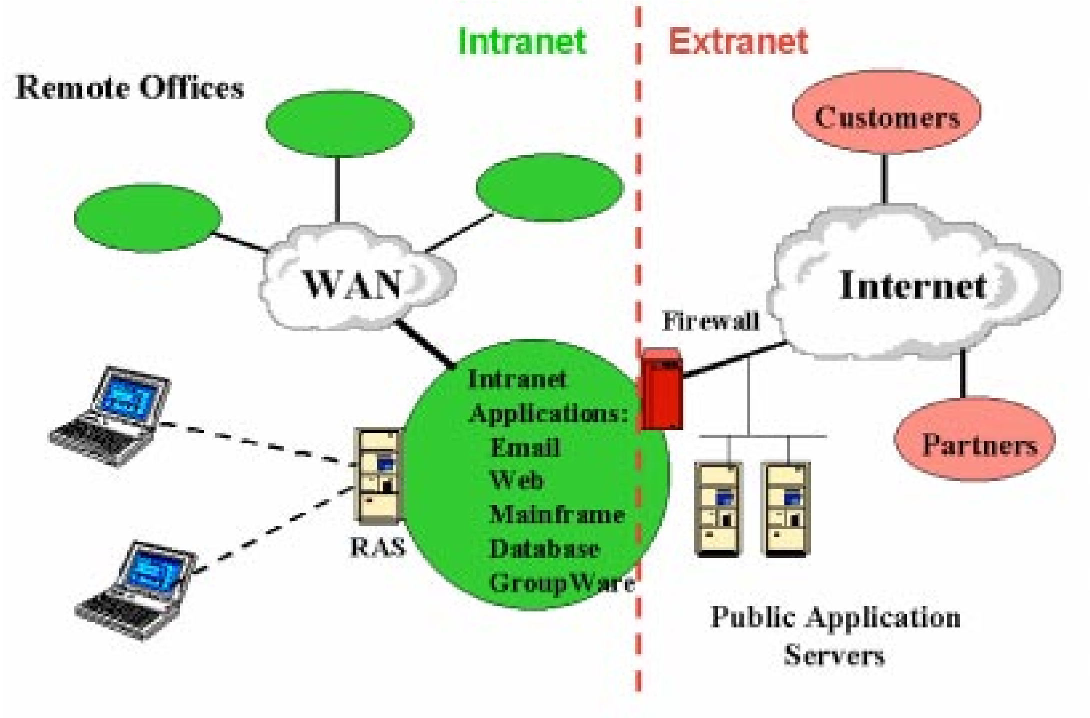
The Opportunity of Virtual Private Networking

A major objective of most IT organizations is to gain competitive advantage by providing more direct and cost-effective means of communicating with critical communities of interest. In the past decade, there has been a steady evolution of infrastructure and security technologies designed to meet this objective.

The emergence of the commercial Internet in the mid-1990s offered the potential of delivering the most effective means of communicating with worldwide communities of interest. The Internet's global infrastructure presented an intriguing alternative to more costly and less extensive Value Added Network (VAN) infrastructure. However, Internet security technology had not yet evolved to enable the level of interactive commerce with customers and partners achieved on proprietary VANs. Firewall technology allowed companies to connect and protect – connect to the Internet and protect company data assets from intruders. The firewall's defensive design, at this time, did not support Internet-based remote access to protected networks. Database, mainframe, GroupWare, and Web applications that provide essential data for key business processes could not be deployed to the remote user over the Internet.

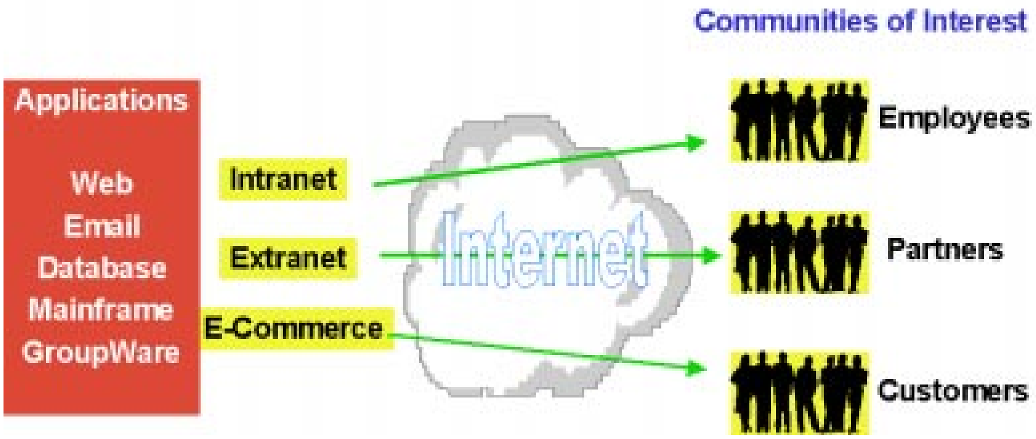
Companies also continued to rely on private networking services, rather than the Internet, when delivering application services to the employee base. Throughout the 1990s, Wide Area Networking (WAN) services remained the preferred infrastructure for connecting remote offices, while remote dial access service for the individual users was achieved by building modem banks and remote access servers on trusted networks. Again, the firewall gateway to the Internet did not have the functionality required to support these remote users.

With the absence of a security technology that enables secure Internet-based business communications, today's enterprise networking architecture consists of a hybrid of VAN, WAN, and Internet networking. The architecture is segmented into private and public spheres, with perimeter firewalls representing the line of demarcation between the two. Private WANs and RAS servers provide private transport services for employee-based Intranet applications, while the Internet is utilized for outbound access and hosting public application servers. This segmentation of private and public wide-area network infrastructure increases costs and limits the scaleability of enterprise applications.



Today's Enterprise Architecture – private and public segmentation increases cost of infrastructure and adds complexity to application environments.

Virtual Private Networking (VPN) is the security technology that will enable companies to leverage the Internet as private enterprise backbone infrastructure. Much is made of the value of Intranets, Extranets, and E-commerce, but until they can be deployed globally, using scaleable network infrastructure, their impact is not fully realized. Using VPNs, all application services hosted on the trusted enterprise can be targeted for worldwide communities of interest using the most cost-effective communications infrastructure available – the Internet.



VPNs enable direct business communications with worldwide communities of interest by leveraging the Internet.

Therefore, a VPN can be defined as *using the infrastructure of the Internet to provide secure access to applications and corporate network resources for remote employees, business partners, and customers*. Migration from proprietary and private networking services cannot be achieved immediately or entirely. However, companies that exploit the cost-effectiveness and global reach of the Internet for delivering business applications to valuable communities of interest will rapidly gain competitive advantage.

SmartGate Overview & VPN Architecture

SmartGate is client/server VPN software that enables companies to securely deploy private application services to remote employees, customers, and business partners. SmartGate is specifically designed to address the challenges of deploying and managing large VPN user populations.

Below is a high-level overview of SmartGate. SmartGate's VPN security and key advantages are addressed with more detail in later sections.

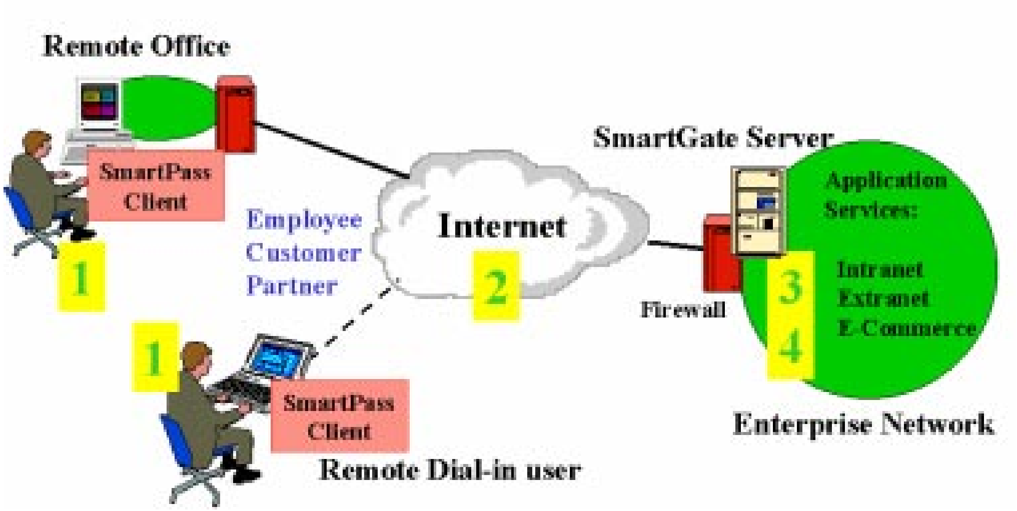
SmartGate Software Components

SmartPass Client – installs on remote user workstations to provide VPN connection services to the SmartGate server. SmartPass manages user authentication by interfacing with a variety of tokens. Successful authentication initiates an encrypted data session with the SmartGate server, securing remote application services to private networks.

Supported Operating Systems – Microsoft Windows NT & 95, Macintosh

SmartGate Server – deploys to the Internet perimeter, either on or behind firewalls. SmartGate's server manages authentication token deployment and registration, VPN session encryption, user connection privileges, and event logging.

Supported Operating Systems – Windows NT, Sun Solaris, BSDI, HP-UX



Numbers correspond to SmartGate VPN Security Summary below.

SmartGate VPN Security Summary

1. **Authentication** – SmartGate ensures the identity of authorized SmartPass users by requiring them to enter an access code and present a token device. SmartGate also verifies that the VPN connection is being established with the intended application by authenticating the SmartGate server.

2. **Data Encryption** – SmartGate keeps application data private while traversing the Internet by encrypting session data passed between the SmartPass client and SmartGate server.

3. **User Access Control** – SmartGate regulates authorized user access to specific trusted network application resources.

4. **Event Logging** – SmartGate records critical SmartPass user connection activity.

SmartGate Advantage Summary

Flexible Integration – SmartGate installs on firewall platforms or a stand-alone platform behind firewalls (on trusted network). SmartGate also offers the choice of integrated authentication components or the use of third-party authentication systems, including SecurID/ACE and RADIUS.

Low-cost and Rapid Deployment - SmartGate enables thousands of remote users to electronically enroll and register authentication tokens with the SmartGate server in minutes.

Ease-of-use – SmartPass users enter an access code to start SmartGate connections. All other security and configuration details are transparent to the end-user.

Remote VPN Client Management – All SmartPass client configuration changes are performed centrally at the SmartGate server and pushed to SmartPass upon the start of new session requests.

Enterprise VPN Management – SmartGate features a Windows-based VPN management console, called SmartAdmin, that enables secure, remote administration of multiple SmartGate servers. SmartAdmin has database functionality for productive user management.

SmartGate VPN Security

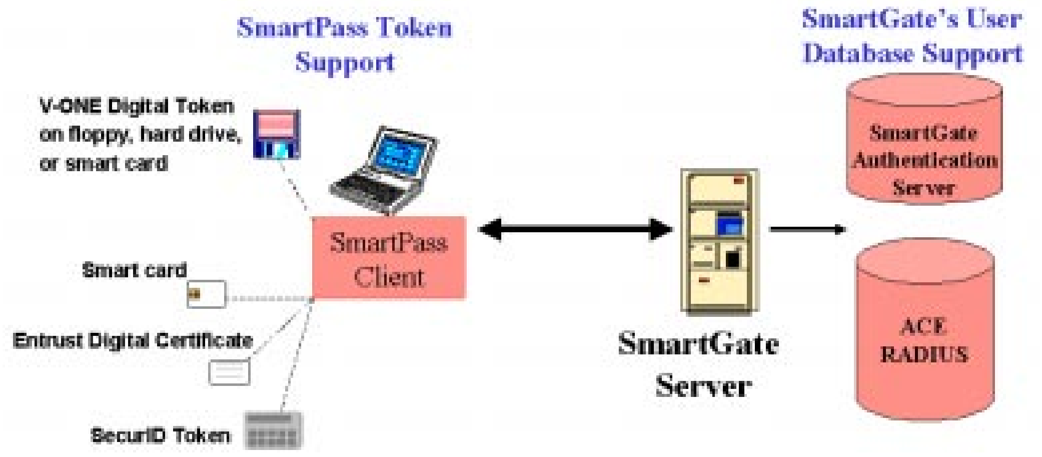
SmartGate Authentication

There are millions of individuals and organizations with access to the Internet. Providing secure Internet access to private business applications requires authorized users to prove their identity before establishing sessions. Likewise, there are thousands (possibly millions) of application servers feeding data to the Internet. Users establishing Internet-based connections with mission critical applications must be assured that they are connecting to an authorized application server. Successfully establishing user identity, then authenticating the user to a remote application and the application to the user constitute a strong model for VPN authentication.

SmartGate's authentication system meets all requirements for strong authentication:

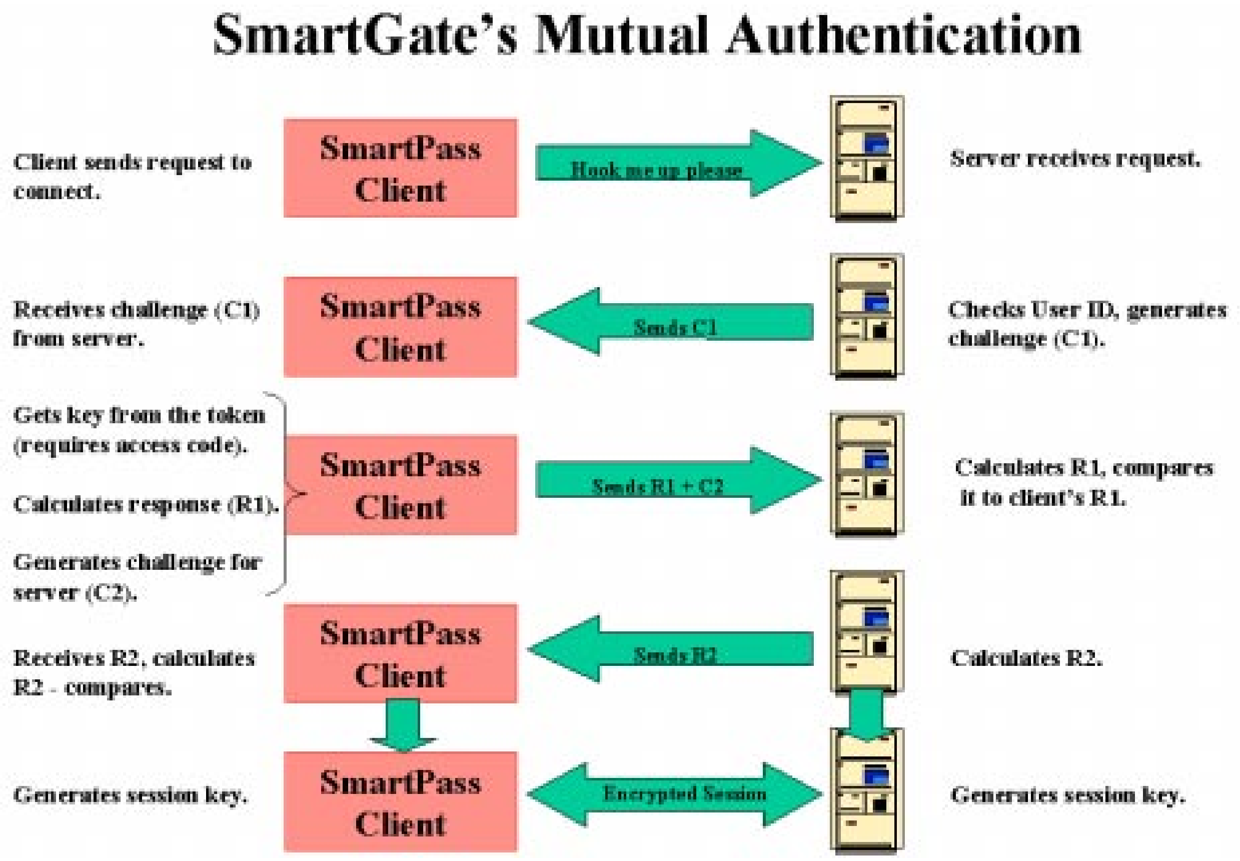
- Two-factor user identification – verifies the identity of an authorized user by something they know, an access code, and something they have, a token.

- Two-way (Mutual) Authentication - authenticates both SmartPass client user and the SmartGate server to ensure that authorized users are establishing VPN sessions with the intended application environment.


SmartPass Token Support
SmartGate's User Database Support
V-ONE Digital Token on floppy, hard drive, or smart card
Smart card
Entrust Digital Certificate
SecurID Token
SmartPass Client
SmartGate Server
SmartGate Authentication Server
ACE RADIUS

SmartGate's integrated authentication includes the use of a digital token, a software emulation of a smart card, and a SmartGate user database

SmartGate authentication features a digital token to identify remote users, and a user database on the SmartGate server side. This integrated authentication system allows a complete VPN solution to be deployed with a single product. SmartGate also supports third-party authentication systems, including the ACE Server/SecurID system from Security Dynamics and RADIUS. SmartGate's mutual authentication process increases the strength of these third-party systems, making them better suited for Internet-based VPN connections.


SmartGate's Mutual Authentication
Client sends request to connect.
SmartPass Client
Hook me up please
Server receives request.
Receives challenge (C1) from server.
SmartPass Client
Sends C1
Checks User ID, generates challenge (C1).
Gets key from the token (requires access code).
Calculates response (R1).
Generates challenge for server (C2).
SmartPass Client
Sends R1 + C2
Calculates R1, compares it to client's R1.
Receives R2, calculates R2 - compares.
SmartPass Client
Sends R2
Calculates R2.
Generates session key.
SmartPass Client
Encrypted Session
Generates session key.

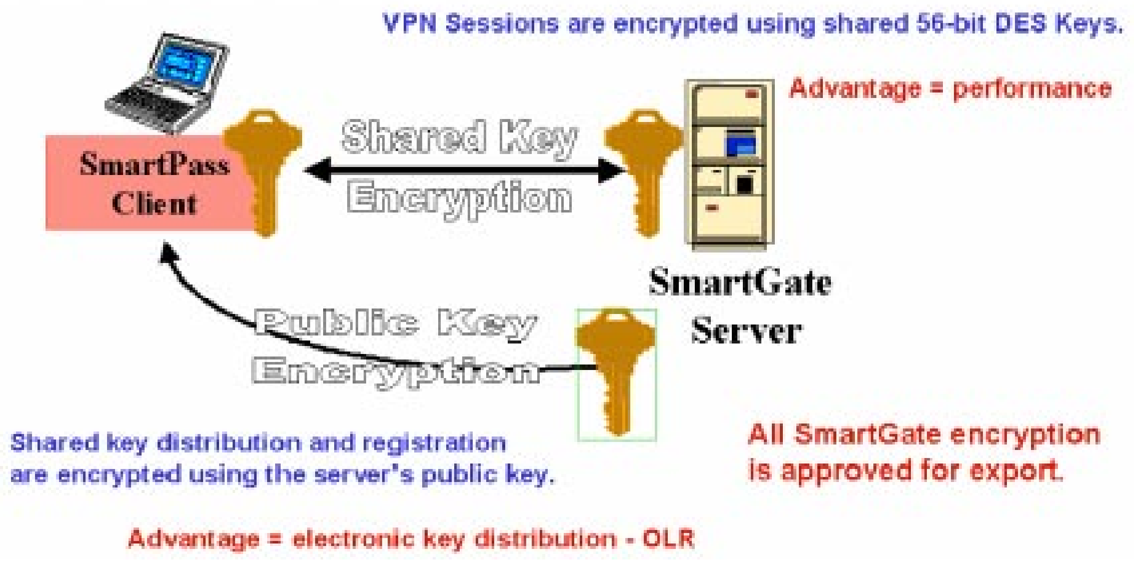
SmartGate's mutual authentication verifies the identity of the SmartPass client user and the SmartGate server. As a result, each session has a unique session key based on random data generated during bi-directional challenges.

SmartGate Encryption

The challenge of keeping information private on the Internet is fundamentally addressed by encryption technology. However, applying encryption for practical use presents a set of challenges beyond that of fundamental privacy. Maintaining productive connection performance and scaling the distribution of encryption keys become the major criteria for successfully supporting VPN remote access.

SmartGate solves these problems by applying two different encryption technologies at two different stages of SmartGate VPN deployment. Public key encryption is used for the SmartGate server's initial (one-time) key distribution, user enrollment, and token registration. User data and keys exchanged during this *on-line registration (OLR)* process must be kept private while traversing the Internet. Since the remote SmartPass client user has no trust relationship with the server at this point, the SmartGate server must establish privacy by using its public key. SmartGate's application of public key encryption during the OLR process enables thousands of remote users to receive and register their encryption keys securely and electronically. This provides a scaleable solution to the problem of deploying VPN credentials to users on a public network.

The authentication key (digital token) distributed to the SmartPass VPN client is a replica of an identical key created on the SmartGate server during the OLR process. This shared key pair is the basis of SmartGate's VPN session encryption. Shared key encryption is computationally simpler than public key technology, offering performance advantages necessary to support business applications over VPN connections. SmartGate uses 56-bit DES, and optional 3DES (available Q4 1998), to encrypt sessions.


VPN Sessions are encrypted using shared 56-bit DES Keys.
Advantage = performance
SmartPass Client
Shared Key Encryption
SmartGate Server
Public Key Encryption
Shared key distribution and registration are encrypted using the server's public key.
All SmartGate encryption is approved for export.
Advantage = electronic key distribution - OLR

SmartGate Access Control

Linking access control to the user’s identity is essential to effectively manage user access to applications. SmartGate enables user-specific access control by having a unique user ID associated with each user’s Access Control List (ACL) entry. Access privileges are only applied once the user has successfully authenticated, ensuring that the access policy has been applied to a specific user. Users can also be managed by assigning them to groups that have common access privileges. Access rules can be defined by destination host, connection service, or the URL file name.

The SmartGate server also contains service proxies that enforce access policy. Proxies apply access policy by taking requests for connections, then making the connection on behalf of the requesting party, based on a set of pre-defined rules. In the case of SmartGate, connection requests originate from the remote SmartPass clients. SmartPass VPN connections terminate at the SmartGate server proxies. The service proxies then complete the connection to the application server and provide application services on behalf of the SmartPass client. SmartGate’s proxy architecture is particularly useful for providing remote application services to customers or partners that should not have direct connection privileges to trusted networks.

Event Logging

Critical events are logged and stored by the server as users are provided remote access VPN services. These include:

- User Added/Deleted
- User Enabled/Disabled
- User Key Changed
- Successful/Unsuccessful User Login
- Session Start/End
- Server Up/Down

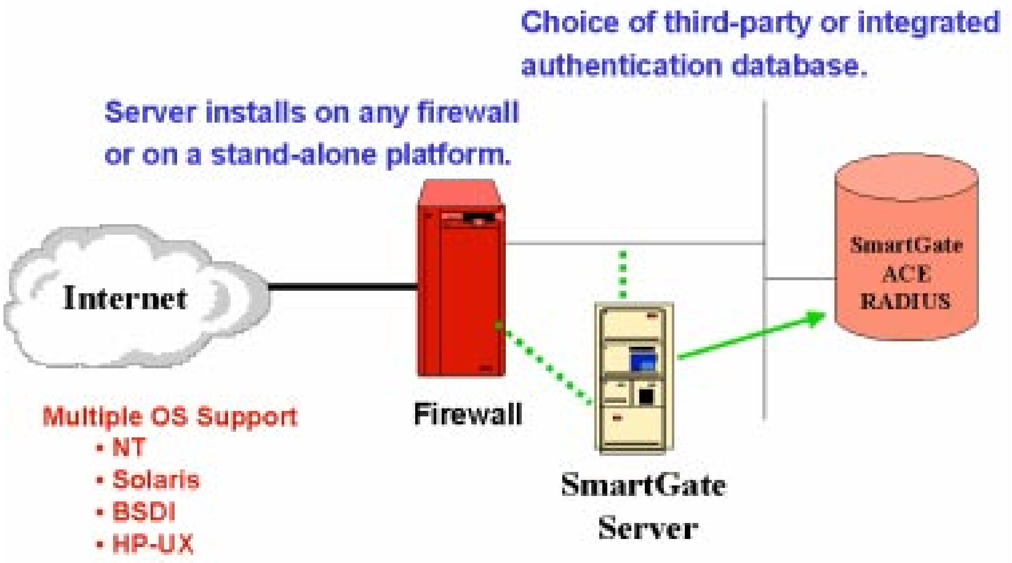
The data captured from logging these events is essential for security audits. It also enables the administrator to review events for troubleshooting purposes.

Key SmartGate Advantages for Deploying and Managing VPNs

Flexible Integration

The ability to integrate VPN solutions seamlessly into the existing enterprise security architecture is a major factor in deploying them successfully. As discussed earlier, most IT organizations have already deployed access and security technologies prior to the evolution of VPN technology. Firewalls are widely deployed to provide perimeter defense for the Internet-connected enterprise. SmartGate is firewall independent VPN software, enabling the ability to deploy a VPN with any existing firewall. SmartGate can be either installed on the same platform as a firewall or installed on a stand-alone system behind (on the trusted side) a firewall.

Remote access to the enterprise network has primarily been accomplished by installing remote access servers (RAS) and modems. RADIUS or ACE user authentication databases are the most widely deployed means of managing the remote dial user's access privileges. SmartGate supports both RADIUS and ACE user databases. This protects investment made in these solutions and eliminates the issue of duplicating network resources.


Choice of third-party or integrated authentication database.
Server installs on any firewall or on a stand-alone platform.
SmartGate
ACE
RADIUS
Internet
Firewall
SmartGate Server
Multiple OS Support
• NT
• Solaris
• BSDI
• HP-UX

Low Cost & Rapid Deployment

Distributing information and processing transactions electronically is becoming a standard means of accomplishing today's business. On-line transactions with remote parties enable complex processes to be accomplished more cost-effectively and faster than "out-of-band" means. SmartGate utilizes on-line processing when handling the challenge of distributing VPN access credentials to large populations of remote users. SmartGate's On-line Registration (OLR) completes the task of distributing a unique digital identity to each SmartPass client user (the V-ONE digital authentication token described earlier) and registering it with the SmartGate server.

As users register with the SmartGate server, they provide information that will assist the VPN administrator when managing their access privileges. For example, a department code or company name can be associated with specific access groups to assign a common access rule. The OLR user information form can be customized to capture information appropriate for each VPN deployment. Remote users register using their Web browser.

Using SmartGate's OLR enables companies to deploy VPN remote access to thousands of users in minutes. The entire OLR process takes remote users less than ten minutes to complete. The steps used to complete the OLR process are described below:

SmartGate's On-Line Registration Process

Step 1 The user downloads an "installation pack". This includes the complete SmartGate client software, plus configuration files which include the location of the SmartGate server, and the server's public key. The download can be made via the Web, FTP, or loaded from a floppy disk.

Step 2 The user extracts the installation pack and runs a Windows installation wizard.

Step 3 The wizard asks the user to perform a random mouse movement. Random data from the mouse movement and several other variables are used to generate a random number.

Step 4 The OLR application connects to the SmartGATE server as defined in the OLR configuration file (which was distributed with the OLR installation pack). This connection is secured with the server's public key.

Step 5 Using the random number generated in 4 and some inputs from the server, the SmartPass client and the SmartGate server securely generate a shared secret key pair.

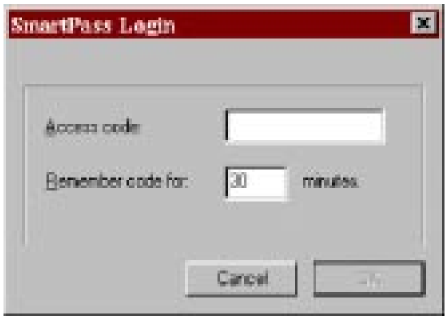
Step 6 The client downloads a second configuration file from the server. This file is used to generate a registration form for capturing user details. The user must fill in all fields before proceeding. The contents of each field in the form are sent back to the server where they are entered into the user database with a corresponding user ID.

V-ONE On-line Registration Technical Abstract (from U.S. Patent 5784463)

ABSTRACT: A shared secret key distribution system which enables secure on-line registration for services provided by an application server through an application level security system or firewall utilizes an authentication token containing a server public key. The server public key is used to encrypt a client-generated portion of the shared secret key, and the encrypted client-generated key is sent to the server where it is recovered using a private key held by the server and combined with a server generated portion of the shared secret key to form the shared secret key. The server generated portion of the shared secret key is then encrypted by the client-generated portion of the shared secret key and transmitted to the client for recovery and combination with the client-generated portion of the shared secret key, at which time both the client and server are in possession of the shared secret key, which can then be used for mutual authentication and development of session keys to secure subsequent communications. The session keys can be used to provide dynamic configuration of a client system to provide for different or changing user entitlements.

Ease-of-Use – SmartPass Clients

The opportunity of providing Internet-based access to enterprise business applications is attractive, however, the challenge of supporting hundreds or possibly thousands of remote VPN client users is significant. V-ONE's SmartPass VPN client is designed to take the technical aspects of establishing VPN connections out of the hands of non-technical remote users. SmartPass installation is performed using the Windows Wizard installation program - a simple tool familiar to most Windows users. Once installed, SmartPass is pre-configured to establish connections with the SmartGate server, eliminating the need for users to enter IP addresses or make other desktop configuration changes.



SmartPass Login

Access code:

Remember code for: 30 minutes.

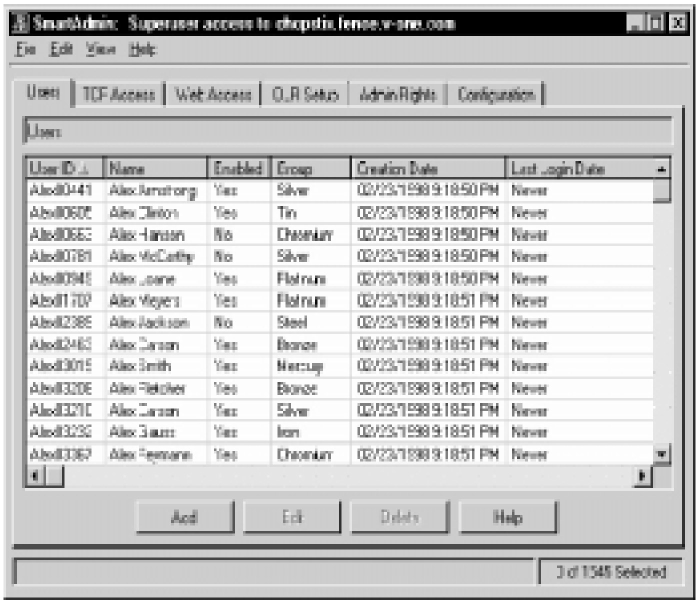
SmartPass users enter an access code to verify their ownership of a registered authentication token. All other SmartPass functions are transparent to the end user.

Centralized VPN Client Management

Managing hundreds or thousands of remote software users is not easy unless the right tools are provided for the challenge. All SmartPass client configuration changes are performed centrally at the SmartGate server and pushed to SmartPass upon the start of new session requests. If changes are applied to groups of users, or even the entire SmartGate VPN population, the update is propagated automatically by this *dynamic reconfiguration* capability. Literally thousands SmartPass client changes can be made in the amount of time it takes to change the access rule.

Enterprise VPN Management

SmartAdmin addresses the issues of managing VPN policy over large enterprise networks. For a VPN solution to be considered "enterprise ready", the ability to manage the entire VPN software base from a central console is imperative. SmartAdmin provides the ability to remotely manage multiple SmartGate servers from anywhere in the world. SmartAdmin sessions to the SmartGate are secured using an authenticated and encrypted SmartGate VPN connection.



User ID	Name	Enabled	Group	Creation Date	Last Login Date
Alex0441	Alex Armstrong	Yes	Silver	02/23/1998 9:18:50 PM	Never
Alex0605	Alex Clinton	Yes	Tin	02/23/1998 9:18:50 PM	Never
Alex0663	Alex Hanson	No	Chromium	02/23/1998 9:18:50 PM	Never
Alex0781	Alex McCarthy	No	Silver	02/23/1998 9:18:50 PM	Never
Alex0945	Alex Loane	Yes	Platinum	02/23/1998 9:18:50 PM	Never
Alex1709	Alex Meyers	Yes	Platinum	02/23/1998 9:18:51 PM	Never
Alex2385	Alex Jackson	No	Steel	02/23/1998 9:18:51 PM	Never
Alex2463	Alex Carson	Yes	Bronze	02/23/1998 9:18:51 PM	Never
Alex3015	Alex Smith	Yes	Mercury	02/23/1998 9:18:51 PM	Never
Alex3208	Alex Fletcher	Yes	Bronze	02/23/1998 9:18:51 PM	Never
Alex3210	Alex Carson	Yes	Silver	02/23/1998 9:18:51 PM	Never
Alex3232	Alex Gauss	Yes	Iron	02/23/1998 9:18:51 PM	Never
Alex3362	Alex Feemane	Yes	Chromium	02/23/1998 9:18:51 PM	Never

SmartAdmin is SmartGate's graphic management console. SmartAdmin enables remote administration of SmartGate servers from a Windows 95 or NT platform.

Managing the VPN user populations quickly and productively are also challenges addressed by SmartAdmin, SmartGate's Windows-based VPN management console. SmartAdmin enables administrators to manage users by groups and subgroups. Database functionality, including the ability to sort, filter, and find user entries increases the administrator's efficiency when managing large user populations.

SmartAdmin also allows VPN managers to delegate various levels of user management to multiple administrators. This distributed management model decreases the number of changes required from the central VPN manager, and defers them to administrators more closely aligned with individual user groups. Administrative privileges are delegated according to the following levels:

- ***Minimal*** - Administrators at this level can only enable/disable users and edit a user's name in the event of a name change or a typographical error. Administrators at this level may also be restricted to administering only certain groups.

- ***Standard*** - Administrators at this level have full access to user data. In addition to those rights provided at the minimal level, administrators can change authentication keys, add and delete users, and edit access permissions. Access at this level may be limited to certain groups.

- ***Superuser*** - Administrators at this level have access to all settings. In addition to the privileges of the standard administrator, superusers can assign administrator levels, change SmartGate configuration settings, and create/edit the OLR

Conclusion

The opportunity Virtual Private Networking presents for improving worldwide business communications is tremendous. VPN technology must address security risks associated with Internet-based commerce, and the practical management issues of servicing remote users in order to fulfill the opportunity. V-ONE has been helping our customers deploy major VPN implementations since 1994. SmartGate has been designed to address our customers' requirements to successfully deliver secure remote access to mission critical information.

For more information regarding SmartGate, please contact V-ONE at:

20250 Century Blvd., Ste. 300
Germantown, MD 20874
301-515-5200 x5502
301-515-5280 Fax
sales@v-one.com

Download a free evaluation copy of SmartGate at www.v-one.com