

Using a VPN Client Deployment Tool

How to make the most of today's advanced remote access technology.

intel®

CONTENTS

Executive Summary	3
Is there a VPN in Your Future?	3
Importance of remote access	3
Economic benefits of VPN	3
Strategic considerations	4
VPN Deployment	4
Making secure connections	4
Client deployment issues	5
For the user	5
For the network manager	5
Role of the Client Deployment Tool	5
Advantages of a VCDT	5
The Intel solution	6
How it works	6
Conclusion	7
For more information	7

Executive Summary

Virtual Private Networks (VPNs) are today's evolution of the secure WAN link, offering an inexpensive way to for enterprises to provide remote access to network resources. For many enterprises, these resources are hosted at the site of an Application Service Provider (ASP) or Hosted Services Provider (HSP). But whether the enterprise or service provider is responsible for maintaining the VPN infrastructure, one aspect of the operation is typically a major challenge: distributing the necessary client software to potentially thousands of remote users or subscribers.

The answer is a new generation of VPN Client Deployment Tool (VCDT). With a proper VCDT, the enterprise or service provider can easily and efficiently handle the initial set-up, and then make user changes and configuration updates on an ongoing basis. For the end-user, the process can be as simple as clicking on a link in an email to initiate automatic client installation.

This paper examines the current state of VPN technology and deployment, providing a detailed description of the uses and benefits of a VCDT. It should be of interest to network managers at service provider sites or enterprise IT data centers.

Is there a VPN in Your Future?

Importance of remote access

More and more, people expect to be in touch with their workplaces on demand. Individuals working at branch offices or traveling in remote parts of the world expect the same access to information as their colleagues using the corporate LAN and its resources in the home office. They recognize, quite rightly, that this type of access can lead to huge productivity gains.

Dial-up remote access has long been the principal technology for achieving this goal. With the phenomenal growth of the Internet, companies have begun taking advantage of the cost savings that can be gained through Virtual Private Networks (VPNs). By using the Internet as a common networking environment, companies have dramatically reduced the costs of connecting their remote personnel. Today, enterprises often rely on service providers to design a remote access solution for them, using VPN equipment deployed at the service provider's site.

VPNs offer dedicated, secure paths, or tunnels, to reconcile the public nature of the Internet infrastructure with the need for security to facilitate e-Business. Products are now available that tunnel and encrypt data for reliably secure passage. As a result, it is only reasonable to expect that more and more companies will be taking advantage of the favorable economics and other benefits provided by Virtual Private Networks.

Economic benefits of VPNs

For telecommuters near a company headquarters, who can access the corporate network with just a local phone call, the public-switch telephone network (PSTN) is still the most cost-effective way to go. However, whenever connectivity would require long-distance calls to the home office, even via a "toll free" or freephone number, VPN technology would be far more economical.

Instead of making a long-distance call to company headquarters, the user simply makes a flat-tariff call to their local Internet Service Provider (ISP). The company avoids long-distance charges and/or the cost of maintaining a toll free/ freephone account. In effect, the cost of Internet infrastructure is shared among the many companies who use it, somewhat like a huge, cooperatively owned WAN.

Service providers can create an additional revenue stream by offering managed VPN solutions. With VPNs, the service provider has a way to save time, money and complexity while providing secure, Web-based access to applications and other hosted resources.

Strategic considerations

Companies are realizing that remote access is more than a tactic to keep business travelers in touch with their offices. It is a strategic necessity in the increasingly competitive global economy. And, as enterprises outsource a growing array of network services, from applications to data warehousing, they need a way to provide secure, authenticated access for users around the world.

Beyond lowering the cost of remote access, VPNs have their own strategic implications. First, they provide access from anywhere the Internet reaches. Second, they help enable a new generation of rich, flexible communications. But perhaps their greatest value is security.

Even before the advent of the Internet, companies secured their WAN connections in order to safeguard sensitive information. These protected links were static, remaining in place, with users often competing for the available bandwidth. Today, VPNs are the new state of the art in communications security, allowing any authorized individual to establish their own secure connection on the fly, at a moment's notice. As such, VPNs change the way people do their work, much as fax and email communications have in the past.

The bottom line is this: if an organization or service provider isn't already using Virtual Private Networking, it probably will in the near future. When that happens, deployment will become a key consideration.

VPN Deployment

Making secure connections

A VPN network consists of authenticated and encrypted tunnels over the Internet (or other shared data network). The tunnels are set up between a network access point, such as a switch or gateway, and a tunnel terminating device on the destination network. The network access point encapsulates packets sent by the mobile or distant user, so that the data can travel securely over the Internet.

The most widely used protocols for encapsulating packets are PPTP (Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) and IPSec (IP Security). IPSec has advantages over the other two, primarily because it allows for various levels of security based on authentication, encryption and key management.

A lightweight IPSec implementation, for example, would provide strong authentication of each packet and ensure data integrity. A higher-overhead implementation would add encryption of the data in the payload. Different encryption methods can be used with IPSec, including the popular Digital Encryption Standard (DES and DES3).

The ability to authenticate network users – preventing one user from masquerading as another – is important to VPN security. The most basic method is to validate passwords using protocols such as Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP). Even more secure solutions involve token cards with time-synchronized keys or the emerging digital certificate technologies.

Most network access points can authenticate clients first by checking internal databases and then, if matches are not found, by accessing external RADIUS servers. Using a centralized RADIUS database for client administration reduces the need to update multiple access points every time a there is a new user or passwords are changed. For example, with RADIUS, users are able to reset their own passwords using the client software on their PCs.

Client deployment issues

VPNs clearly represent a valuable opportunity, enabling an organization to increase its effectiveness and competitiveness, while reducing costs at the same time. Another attraction is the fact that VPNs are platform independent. Any computer that has been set up to run on an IP network can be incorporated into a VPN with no modifications other than the configuration of remote client software.

However, there are significant challenges facing organizations when it comes to deploying this client software. VPNs tend to be geographically dispersed and are often international in scope. Many enterprises or their service providers find they are faced with deploying new technologies in far-flung locations, to thousands of different users. This presents specific challenges for both the user and the network manager.

For the user

Many users are non-technical people such as accounting personnel in remote offices or salespeople with laptops. In addition, remote offices normally lack the IT support that is taken for granted at a headquarters campus. Unless client software is easy to use, with a familiar graphical interface and a minimum of questions to answer, users may have difficulty understanding and configuring the client. In particular, questions pertaining to tunnel set-up can be beyond the scope of most users.

For the network manager

For network managers at ASPs, HSPs or corporate IT departments, the principal issue is the large amount of labor-intensive distribution work that is required, and the associated costs in time and/or

money. The challenges may include distributing client software to each user via floppy disk, along with a password, ID, digital certificate or other shared secret to validate the identity of the sender and receiver. Deployment could involve the set-up of initial security keys, followed by mass mailings to dozens of worldwide locations, complicated by a variety of configurations based on the different network access levels assigned to different categories of employees.

Another issue for the network manager is ongoing management and maintenance of the VPN system. For example, employees routinely change locations or employment, and growth of the organization may require re-assignment of tunnels. The scope of the service provider's work may include this responsibility. The quality of the client software, distribution mechanism and network access points, as well as the way these elements work together, can make a significant difference down the road.

Role of the Client Deployment Tool

Advantages of a VCDT

The overall function of a VPN client deployment tool (VCDT) is to enable faster, simpler deployment and maintenance of the client software. For many organizations, such a tool may remove the only remaining barrier to VPN adoption, allowing the company to take full advantage of today's advanced remote access communications.

The most effective client deployment tools provide advantages for both network managers and users, such as:

- Time savings through initial automated client deployment
- Ease of ongoing client maintenance through file import of user list and hardware configuration information
- Ease of use through an intuitive graphical user interface

The Intel solution

VPN client deployment tools vary significantly. To describe with a meaningful level of detail how a VCDT works, it is necessary to use a specific tool as an example. The Intel® NetStructure™ VPN Client Deployment Tool is used as an example in the sections that follow. In general, this solution is characterized by the use of Web-based technology, rather than floppy disks, for client deployment.

In addition to the deployment tool, Intel also offers a line of Intel® NetStructure™ VPN Gateways, which serve as multi-purpose network access points. The access point(s) and deployment tool are designed to work together in an integrated manner. For instance, the deployment tool can automatically obtain configuration data, including tunnel definitions and authentication set-ups, directly from the gateways.

How it works

For the user

The Intel NetStructure VPN Client Deployment Tool can be used to send fully pre-configured client packages to each individual user via email. The user clicks on an URL contained in the email, logs on – typically with a user ID and password – and downloads one or more self-extracting Zip files. These files automatically launch the Windows* OS-based client application, which self-installs. The user simply reboots to make the client fully functional.

Each software configuration arrives customized for the user's local network, with all of the correct IP addresses in place. No authentication set-up is required, and there is no need for the user to enter the IP address of the local Internet Service Provider, because this information is already included. When changes are needed, users receive individual email notification that an updated configuration is available at a specific URL. They can use any Web browser to log in and download their client software, for initial set-up or updates.

For the network manager

As part of initiating a VPN solution, the manager establishes a centralized server where sets of user names and email addresses are maintained. Thousands of users can be managed per organization. The initial lists can be imported from a variety of different source file types with little text manipulation. In addition, the Intel gateways discover and provide network information, including the IP addresses of any equipment that will be acting as front-end devices for the remote destination networks.

User name and address information is only required to be entered once. A corporation with an office in Paris and London could use a different gateway for each location, but both gateways would employ the same central database. This integrated database, together with Web and email server interfaces in the VCDT, facilitates automatic client software configuration.

For ASPs and other service providers offering secure access to applications or other hosted resources, the VCDT provides a simple, Web-based distribution system – one that can be re-used for any number of customers. There is no need for either the service provider or the customer to collect user laptops for configuration. Instead, the service provider pre-configures a client and places it on a Web server using the VCDT. Simultaneously, the VCDT sends the appropriate URL to subscribers via email.

The Intel solution also allows users to be organized into a tree of user groups that facilitate management. For example, in addition to geographic divisions, users can be tiered according to their job categories and corresponding network access rights, which in turn determine gateway and tunnel assignments. When the administrator selects the group of users to upgrade, VCDT identifies those users that are in need of the upgrade and can distribute the client only to those users.

As new employees are added to the organization, instead of manually entering their configuration data, the enterprise or service provider can assign them to a user group where they will automatically inherit the proper configuration. The inheritance features of the Intel NetStructure VPN Client Deployment Tool let network managers set important parameters such as tunnel assignments and authentication server addresses in one place and apply them to many users. This makes it easier to scale the solution as the organization grows.

For initial client deployment, the tool's GUI enables the manager to automatically build clients from the database, create INI files and send them via email accompanied by predetermined authentication measures. Without a VCDT, authentication usually requires a floppy disk. With the Intel NetStructure VPN Client Deployment Tool, the first time a user connects to the gateway, an X.509 based certificate can be served to the user through a firewall rule, making floppies unnecessary. For added security, the configuration files themselves are encrypted.

Once deployed, configurations continue to support all of the Intel NetStructure VPN Gateway security mechanisms for client updates. These mechanisms include Radius and SecurID* (a widely used proprietary solution), as well as Intel certificates that can be fulfilled automatically over the network.

To summarize, the VCDT automates many types of everyday tasks, including adding, updating users and removing users. It is easy to use with Radius and Intel or third party certificate authorities. The VCDT also makes it easier to adapt to network changes such as the renumbering or merging of networks.

Conclusion

In one sense, Virtual Private Networks are nothing new. After all, a tunnel is simply today's term for an encrypted WAN link. In another sense, they represent a whole new paradigm in remote access communications.

While many people have been resistant in the past to using the Internet for their corporate network access due to security concerns, the newest generation of VPN technology is solving these problems quite effectively. VPN client deployment tools help make this security practical for today's data center environments, automating or eliminating the time-consuming and costly tasks of VPN deployment and management.

The Intel solution, including the Intel NetStructure VPN Client Deployment Tool, saves time and complexity for service providers who are offering managed VPN services, and makes it easier for enterprises to reduce telecommunications costs by routing protected traffic over the Internet.

It's clear that the Internet will become the public communications backbone for everyone in the years ahead. For the business world, the challenge is to also make it selectively private, with the sophisticated network services that most organizations require.

For more information

For more detailed information, please visit:
<http://www.intel.com/network/>

* Third party names and brands are the property of their respective owners.

Information in this document is provided in connection with Intel products. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted by this document. Except as provided in Intel's Terms and Conditions of Sale for such products, Intel assumes no liability whatsoever, and Intel disclaims any express or implied warranty, relating to sale and/or use of Intel products including liability or warranties relating to fitness for a particular purpose, merchantability, or infringement of any patent, copyright or other intellectual property right. Intel products are not intended for use in medical, life saving, or life sustaining applications. Intel may make changes to specifications and product descriptions at anytime, without notice.