Abstract

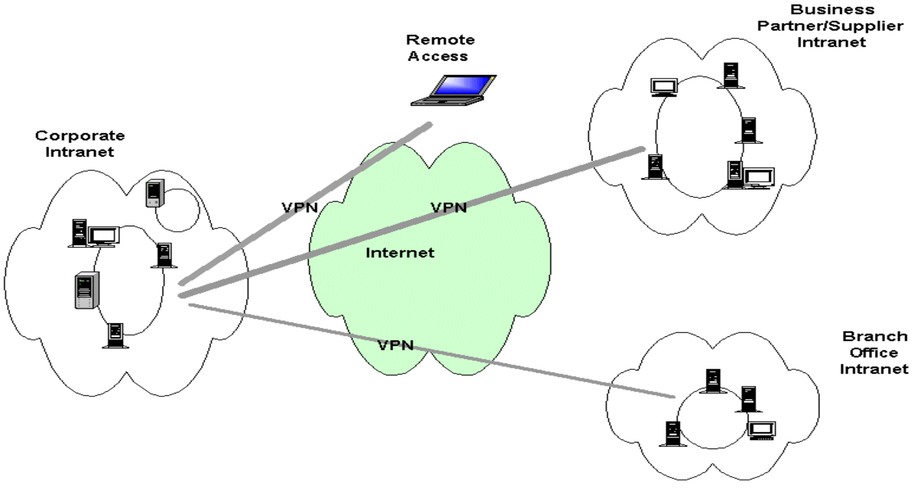
Virtual Private Networks (VPNs) are today becoming the most universal method for remote access. They enable Service Provider to take advantage of the power of the Internet by providing a private tunnel through the public cloud to realize cost savings and productivity enhancements from remote access applications. VPN meets the four key enterprise requirements of *compatibility, security, availability and manageability*. A VPN is an extension of an enterprise's private intranet across a public network (the Internet) creating a secure private connection, essentially through a private tunnel. VPNs securely convey information across the Internet connection remote users, branch offices, and business partners into an extended corporate network [2]. *In this paper I will attempt to give an overview of VPN and its services, their implementation, the three main types of VPNs.*

VPN services

A virtual private network (VPN) consists of a set of geographically disparate sites that can communicate securely over a public or shared infrastructure. IP-based VPNs (IP-VPN) enable business customers seamlessly to receive the same security, connectivity and reliability from any other private network, and can be used to offer the following services:

- *intranet*—connectivity between corporate sites;
- *dial-in access*—business employees can access the corporate network remotely
- *extranet*—secure connectivity between a community of users or business partners whose access is restricted to the resources defined for that community; and
- *internet access*.

VPNs can be built in various ways. Some consist of routers and firewalls that are inter-connected to the physical or logical leased line of carriers and service providers. Others might include a combination of application proxy firewall, encryption, intrusion detection, tunneling, and key management. Some VPNs are managed in-house, while others are outsourced to a service provider. Whether the VPN constitutes remote-access service to an intranet or extranet, a service provider must somehow integrate the VPN services into a common infrastructure. ***Below is sample of end-to-end VPN across the Internet.***



The Opportunity & the Risk of VPN

Remote users dial into a local POP and connect to the corporate network through the Internet. The result is dramatic: significant cost reductions, increased productivity, improved service and anywhere, anytime access. With all its power come risks too. After all, that VPN is tunneling right through the public network and opening your “network doors” to a wide range of users — users that you can’t necessarily see or touch. These users are accessing valuable corporate data assets and conducting mission critical transactions. If the right people are accessing the right information, you couldn’t find a more powerful business tool. But VPN remote access in the wrong hands could be devastating to your e-business.

An Overview of a VPN Implementation

In its simplest form, a VPN connects multiple remote users or remote offices to the enterprise network over the Internet. Whether in support of a traveling employee or a branch office, the approach is similar. The remote user places a call to the local Internet Service Provider (ISP) Point of Presence (POP). The call is then encrypted and tunneled through the Internet, and connected to the destination server on your premises.

VPN Scenarios

There are several primary scenarios for using VPNs, each bringing you the benefits of reduced bandwidth charges, lower network operations costs, simplified administration, reduced capital expenditures, and increased scalability and flexibility. The key challenge for you is to implement the optimal security solution for each application.

Remote User Access

This approach allows remote users to tunnel calls over the Internet. The calls are aggregated onto a remote access server and provided with access to your Local Area Network (LAN) resources. Users can connect over analog modems or using Basic Rate ISDN (BRI) terminal adapters. They can be based in a fixed location — such as telecommuters or contractors — or they can be mobile such as traveling executives or sales representatives. The security challenge in this application is to authenticate users to determine that they are indeed who they claim to be. Since many of the users are mobile, “call-back” techniques are not applicable.

LAN-to-LAN Connectivity

This application reduces the requirement for expensive, leased line solutions. Remote offices consolidate LAN traffic onto a high-speed Internet connection, usually via a multi-protocol router, which provides connectivity to other branch offices and to the enterprise network. The security challenge is to implement both two-factor authentication and session encryption. This approach allows each LAN to be validated for network access while also allowing the virtual connection to be safely encrypted to protect from eavesdropping.

Extranets

Communications between companies are being enhanced through the introduction of extranets, which provide LAN-to-LAN connectivity between you and your business partners, customers, and even suppliers. Extranet applications allow organizations to improve productivity and achieve competitive advantages by streamlining supply chain management, improving customer service, and providing higher quality communications to the distribution channel. Production, order processing, sales and customer support applications are among the most commonly deployed extranet applications. Extranets require varying security levels, and you need the flexibility to dynamically assign multiple security levels.

Authentication: Privacy vs. Security

So, VPNs are private — and the encrypted tunnel protects your data as it travels across the public network. But does not necessarily equal security. To be completely secure, there's still one more thing that you need to beware of — that is the authenticity of users. When a remote user accesses your corporate network, how do you know that he is who he says he is? Without enhanced security, you don't know — not for sure anyway. In an attempt to identify users, many VPNs are protected merely by passwords. However, passwords alone cannot ensure secure remote access because they are a weak form of security. Passwords are easily guessed, stolen or otherwise compromised. And if a password is compromised you have no idea who is at the other end of your VPN.

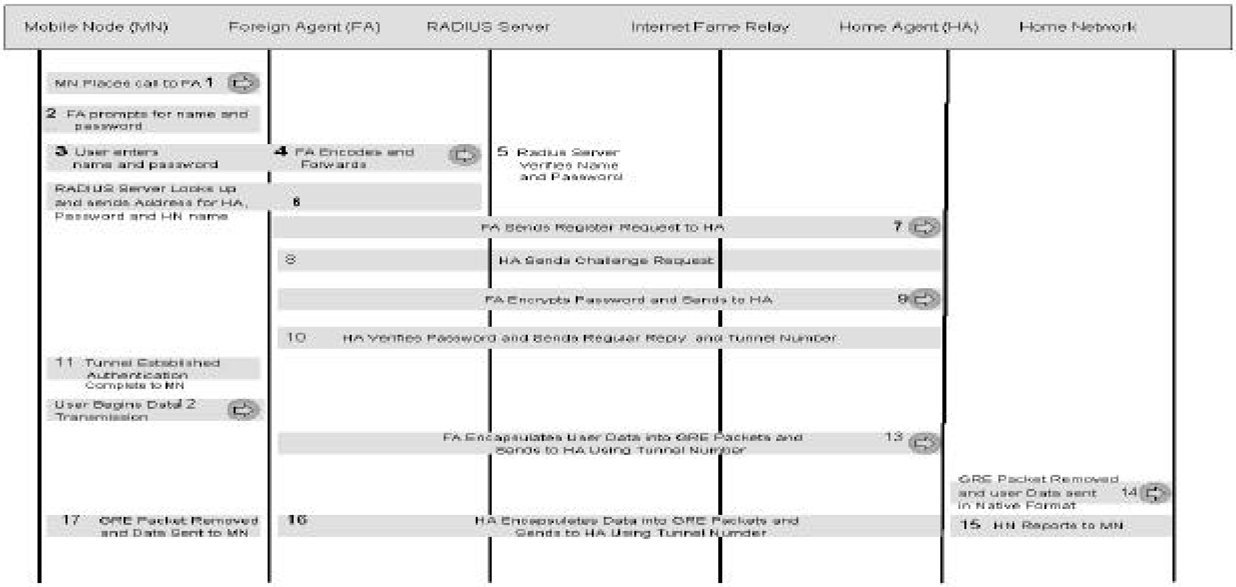
VPN Authentication Choices

The cornerstone to VPN security is authentication — the act of identifying and verifying the authenticity of users before they gain access to critical data assets and resources. One would want to select from varying levels of authentication strength based on the value or sensitivity of the information that you're protecting, balanced against other considerations like usability, deployment, and budget.

All end-to-end tunneling protocols have up to four special entities-depending on where tunnels originate and terminate. These entities are as follows:

- The *Mobile Node* is the remote client or server initiating the VPN session. Mobile Nodes may be stationary (attached to a LAN), or truly mobile (a traveling employee's PC) [2]
- The *Home Network* is the private network containing the resources the Mobile Node wishes to access.
- The *Home Agent* resides in the WAN access equipment at the Mobile Node's Home Network site or in the destination server.
- A special *Foreign Agent*, which acts on behalf of a Mobile Node or Home Network client or server, resides in the WAN access equipment at the local site or service provider POP-at either or both ends of the connection.

See diagram on mobile node and home network handshaking exchanges on tunnel. It references the above description.


Mobile Node (MN)
Foreign Agent (FA)
RADIUS Server
Internet Fame Relay
Home Agent (HA)
Home Network
MN Places call to FA 1
2 FA prompts for name and password
3 User enters name and password
4 FA Encodes and Forwards
5 Radius Server Verifies Name and Password
RADIUS Server Looks up and sends Address for HA, Password and HN name
6
FA Sends Register Request to HA
7
8
HA Sends Challenge Request
FA Encrypts Password and Sends to HA
9
10 HA Verifies Password and Sends Reguler Reply and Tunnel Number
11 Tunnel Established Authentication Complete to MN
User Begins Data 12 Transmission
FA Encapsulates User Data into GRE Packets and Sends to HA Using Tunnel Number
13
GRE Packet Removed and user Data sent in Native Format
14
15 HN Reports to MN
16
HA Encapsuletes Data into GRE Packets and Sends to HA Using Tunnel Number
17 GRE Packet Removed and Data Sent to MN

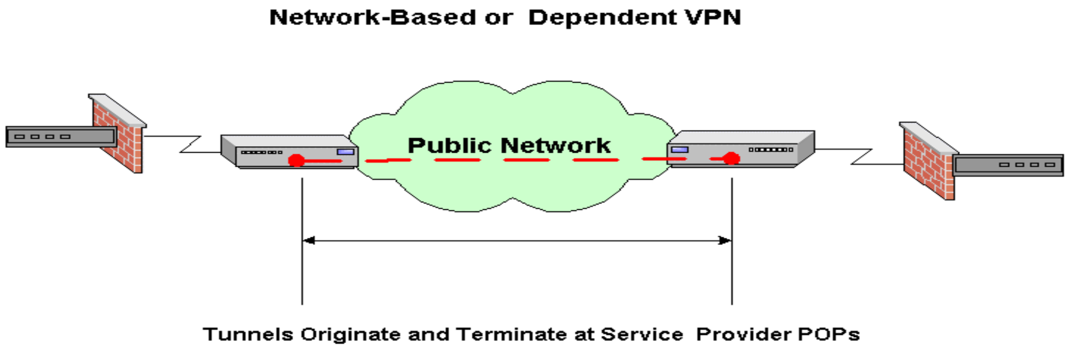
Tunnel Protocol Handshaking exchange

The VPN Infrastructure and Architecture

VPN vary form one organization to another depending on the uniqueness of the enterprise networks. Creating a competitive VPN requires an understanding of the potential differences as well as specific segment requirements. There are three alternative VPN architectures: Network-based or Dependent VPN, CPE-based or Independent VPN, and hybrid VPN.

Network-based or Dependent VPN

Network-based or Dependent VPN exist when the service provider offers the complete VPN solution and serves as a fully outsourced solution. Here, the service provider handles all tunneling, security performance and management requirements for the enterprise organization. This makes the architecture dependent on the service provider. This approach places the IP-VPN network intelligence in a smaller number of devices at the edge of the network and aggregating traffic from CPE devices, the VPN service becomes much more scalable. By centralizing the operation of the IP-VPN network, the service provider achieves much lower operations costs than the collective operations costs of each enterprise managing its own CPE-based solution. The lower cost of operations allows the service provider to provide more competitively priced services.


Network-Based or Dependent VPN
Public Network
Tunnels Originate and Terminate at Service Provider POPs

Network-based or Dependent VPNs originate and terminate on equipment within the service provider POPs. End user customers handle only nature native IP, IPX or other network traffic.

Policy management resources such as directory servers become a shared resource in a NW-VPN, resulting in better price performance. Also, the economies of scale allow the service provider to invest in the right expertise and deliver more rapid service creation.

In short, NW-VPNs allow service providers to offer managed VPN services that:

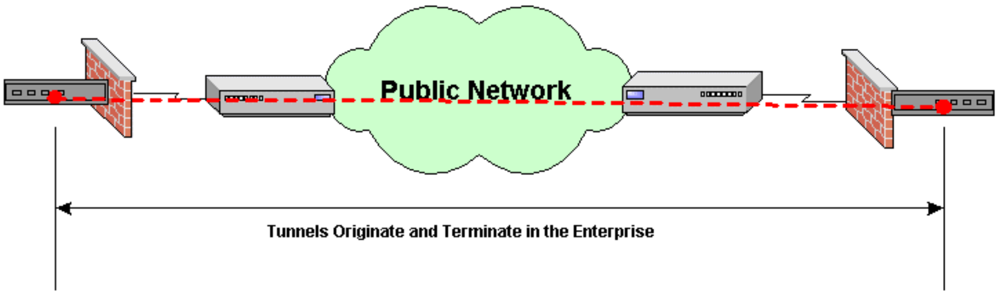
- lower the cost of operations for deploying new IP services
- leverage existing assets to maximize revenue creation
- are highly scaleable
- allow rapid service creation.

CPE-based or Independent VPN

CPE-based or Independent VPN is based on customer edge device or router. This means that the CPE device, that is, customer edge router, plays the key role. The enterprise handles all VPN requirements with its own equipment, relegating the service provider to the role of a WAN carrier. Here, the service provider sees only IP, frame relay or ATM traffic, and does no concern it self whether the traffic is for the Internet or for the VPN. The CPE provides VPN management, provisioning, routing tables, traffic control, and security. With a CPE-based or Independent VPN, all participating sites exchange traffic with a local POP. All traffic is encapsulated and decapsulated, and optionally encrypted and decrypted, at the organization's sites.

This IP-VPN approach provides limited scalability and little or no opportunities for differentiated service offerings, class of service traffic management or service billing in the service provider network. Even with its limitations, CPE-based VPNs remain a practical and effective solution, and are indispensable in extending the VPN domain over the public Internet, or in guaranteeing the a high level of end-to-end security by performing tunnelling and encryption within the CPE. CPE-based VPNs have allowed service providers to enter the IP-VPN market without any direct impact on their backbone networks. Some of the CPE devices used by service providers offer end-to-end QOS to support bandwidth management on the upstream component of the last mile link, as well as capability for translating and signaling QOS to the IP core network.

CPE-Based or Independent VPN

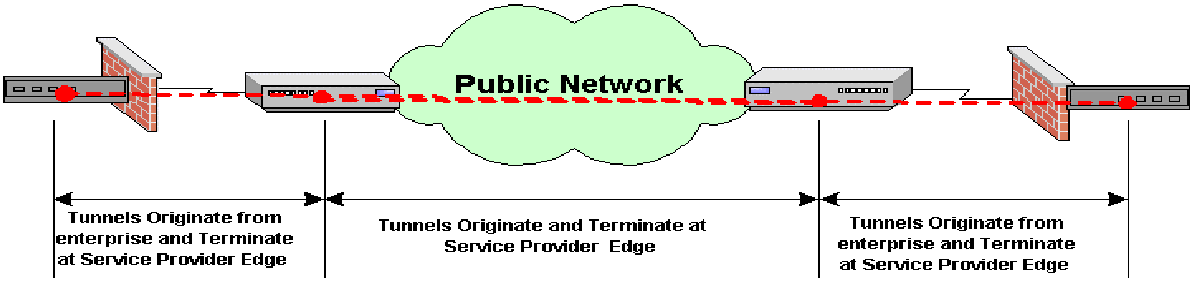


CPE-based or Independent VPns originate and terminate on equipment at customer locations. The enterprise is totally responsible for the VPN and uses service providers merely to transport IP traffic.

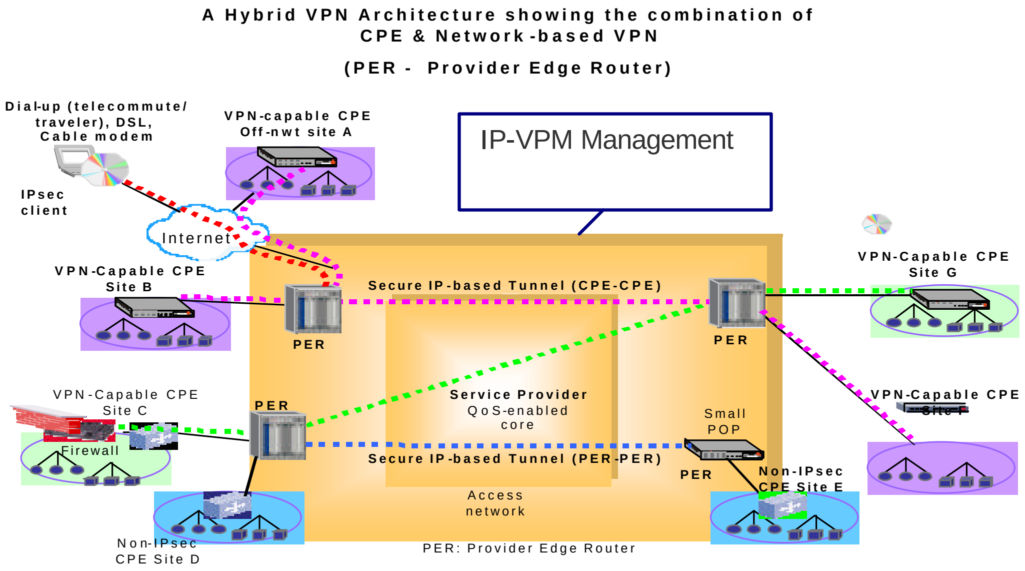
Hybrid VPN

Hybrid VPN involves a combination of network-based (dependent) VPN and CPE-based (independent) VPN sites. Hence, a Hybrid VPN (hybrid architecture) combines the advantages of CPE-based VPN with Network-based VPN. The scenario is clear when an organization could not fully provide an outsourced solution because some sites are beyond the primary service provider's area. The hybrid approach allows the service provider to handle all VPN-specific requirements for those sites within their service area, and at same time, allowing the VPN-capable CPE to provide all VPN-specific functionality. Essentially, it is the same as Network-based VPN, but with encryption end-to-end from customer-site to customer-site, instead of only from provider-edge to provider-edge. This is achieved by placing IPSec CPE at the customer site, and switching packets from one IPSec tunnel to another at the provider edge router (PER).

Hybrid VPN


Public Network
Tunnels Originate from enterprise and Terminate at Service Provider Edge
Tunnels Originate and Terminate at Service Provider Edge
Tunnels Originate from enterprise and Terminate at Service Provider Edge

Below is an example of a fully implemented Hybrid VPN Architecture



A Hybrid VPN Architecture showing the combination of CPE & Network-based VPN

(PER - Provider Edge Router)

While Firewall implementation help to prevent data from leaving and entering an enterprise by unauthorized users, they do little to protect against threat within the Internet. Sensitive data such as user names, passwords, account numbers, financial and personal medical information, server addresses, etc. is visible to hackers and to potential e-criminals over the Internet. This is where the benefits of VPN is seen. A VPN, at its core, is a fairly simple concept—the ability to use the shared, public Internet in a secure manner as if it were a private network. With a VPN, users encrypt their data and their identities to prevent unauthorized people or computers from looking at the data or from tampering with the data. Today, almost all new access routers are VPN-capable and makes building secure networks easier.

References:

1. Virtual Private Networks - *A Resource Guide for Service Providers,* **Lucent Technologies, Bell Labs.**
2. **IBM** Firewall, Server and Client Solutions, *A Comprehensive Guide to Virtual Private Networks*, Volume 1: Martin Murhammer, Tim Bourne, Tomas Gaidosch, Charles Kunzinger, Laura Rademacher, Andreas Weinfurter.
3. Implementing a Secure Virtual Private Network, **RSA Security Inc**.
4. **Cisco** Enterprise Solutions – Virtual Enterprise Networks http://www.cisco.com/warp/public/779/largeent/learn/technologies/VPNs.htm
5. IP Virtual Private Networking – Carrier Managed IP Virtual Private Networking http://www.nortelnetworks.com/solutions/ip_vpn/carrier.html