SecureVCN™ – A Carrier-class VPN Service without Truck Rolls

Dr. Hasan Alkhatib*

1. Increasing requirements on VPN solutions

Business organizations today enjoy unprece -dented connectivity over the Internet that directly affects their bottom line and their top line. Connectivity increases productivity and reduces cost of operations. It eliminates barriers resulting from distance and integrates the world. Never -theless, businesses today face a challenging trade-off between securing their corporate assets and leveraging this ubiquitous connectivity to improve their operations. The complexity involved in striking a balance between security and connectivity stems from dealing with the problem using methods that are rooted in the tradition of plumbing. Typically, either or both, the physical network and perimeter security devices, such as firewalls, have to be reconfigured to meet this desired balance.

2. IP Dynamics' SecureVCN™

IP Dynamics offers a new breed of networking platforms based on the paradigm of policy-based virtual networks[1] Virtual networks are software networks, where computers with virtual network software drivers coordinate their communications through a hosting, virtual network directory server. The solution eliminates the need for gateways or access servers in customer premises. IP Dynamics' virtual networks are based on virtual domains, simplifying management dramatically and eliminating the need to deal with cumbersome IP addresses. Associated with each virtual network is a set of policies. Policies are provisioned using intuitive symbolic domain names that identify member computers. Policies establish the rules of communication among computers in a virtual network. An administrator can administer these policies on the central

---

* President, CEO and Chairman of IP Dynamics. IP Dynamics is the world leader in secure virtual network solutions. Dr. Alkhatib founded IP Dynamics

1) IP Dynamics policy-based Virtual network technology is based on over ten awarded patents and pending patents.

hosting server through a web-based graphical user interface, GUI. Policies are pushed to end computers for enforcement as computers join a virtual network.

IP Dynamics' first application of its policy -based virtual network paradigm is Secure Virtual Networks, where policies define communication security rules. These security policies are compliant with standard host-to-host IPsec. They include access control rules as well as IPsec authentication and encryption rules. Policies can be defined at a level of granularity of a single computer and a single application.

Virtual networks ride, in a virtual layer, on top of existing physical networks and interoperate with common firewalls, edge routers and existing VPNs, seamlessly. Virtual networks can be setup and torn down in minutes. A service provider can create tens of thousands of secure virtual network overlays on the same hosting server. Computers and users join and leave a secure virtual network at will. A computer, such as a server may reside in a virtual network all the time. Computers in a virtual network appear to each other as if they were in the same physical IP subnet, restoring the full peer-to-peer IP-level semantics among them. As a result, all IP-based applications work in a virtual network, regardless of network and organizational boundaries. This unique break -through capability eliminates barriers encountered in traditional VPNs, when applications cross Network Address Translation (NAT) devices and Firewalls. The entire class of collaborative communication applications falls in this category. This includes applications such as

VoIP, NetMeeting and video-conferencing.

Computers in a virtual network can connect from anywhere to anywhere securely, with fully automated host-to-host IPsec and IKE(the Internet Key Exchange protocol). No physical network reconfiguration is required. No change to firewall security policies is required. And, no cumbersome administration of parameters in every computer is required. The result is unconstrained secure connectivity from anywhere to anywhere with unmatched ease of deployment, ease of management, and ease of use.

The following diagram depicts an installation of a Secure VCN platform by a carrier and illustrates the creation of secure virtual networks as overlays.
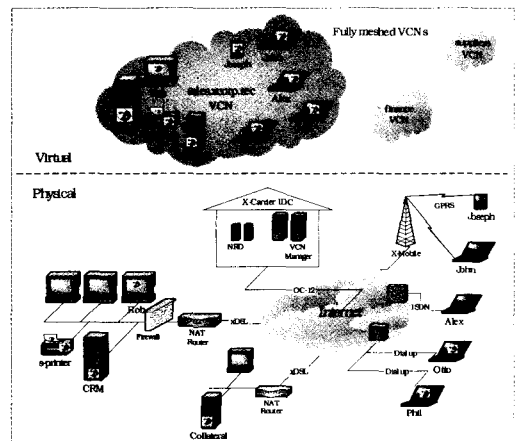
(Figure 1)Carrier Hosted Secure Virtual Network Services

3. Traditional Carrier VPN Services

As carriers transition towards converged integrated data services, new IP-based services such as VPN services present business opportunities for new revenue streams. Traditional VPN solutions for carriers fall in two classes: network-based and customer premises-based:

3.1 Network-based VPN

Network-based VPN solutions include services like frame relay, ATM virtual circuits, and MPLS-VPN. They have two fundamental advantages for carriers: they enable them to offer customers guaranteed SLAs; and they guarantee the utilization of the carriers' backbone bandwidth, which is a carrier's main reason for being in business.

Network-based VPN on the other hand is limited to the physical territory of a carrier. Enterprises that have a large worldwide footprint cannot meet their connectivity requirements using network-based VPN alone. Furthermore, network-based VPN requires reconfiguring the networks in each customer site, exposing the details of customer networks to carrier personnel, which is an undesirable byproduct of the service. The carrier will unnecessarily get involved with managing customer IP addresses as well, a burden that makes the offering more complicated and costly. Therefore, network-based VPN solutions are suitable for tying together large business sites within a carrier's territory, but are too complicated and expensive to integrate small sites, or to meet requirements of remote access users and extranet VPN services.

3.2 CPE-based VPN

Customer Premises Equipment, CPE VPN use IPsec VPN gateways or SSL-VPN servers. IPsec VPN gateways come as stand-alone or integrated in firewalls. SSL-VPN relies on a web server placed in a customer site to provide access to limited types of back-end services. Clientless SSL VPN is attractive since it eliminates the complex administration chores traditionally associated with IPsec CPE VPN.

To meet customers' requirements that are not met by network-based VPN, many carriers have engaged in managing CPE VPN. IPsec CPE VPN enables integrating customer sites that are beyond the territory of one carrier. It also offers a lower cost alternative to network-based VPN for connecting small business sites to the rest of the private corporate WAN. Both types of CPE VPN enable secure remote access services of corporate assets from the Internet for road-warriors and telecommuters at a cost that is lower than network-based VPN solutions. Nonetheless, to the carrier, this is a managed service, where the equipment is in the customer premises rather than a hosted service, where the equipment is in the carrier premises.

CPE VPN managed services are costly. They require truck-rolls to customer premises, which are often combined with reconfiguring the customers' networks as well as reconfiguring their edge routers and/or firewalls. The cost of deployment of such solutions, and their ongoing management renders them too expensive to most small and medium size businesses. They are also too expensive for enterprises that have a large number of small sites, such as retailers. Carriers' profit margins from managed CPE VPN services are fairly low.

Furthermore, when all is said and done, CPE VPN solutions do not support many IP-based applications that are vital to business customers.

Clientless SSL-VPN supports webified applications only. IPsec CPE VPN does not support IP applications that break over NAT or firewalls. Both types of CPE-VPN do not support peer-to-peer applications, which include emerging (Session Initiation Protocol) SIP-based applications that are vital to carriers' core future business.

4. Next Generation Carrier VPN Services

Secure VCN is an economical alternative for carriers to managed CPE VPN services. It opens new business opportunities for carriers. With the Secure VCN platform carriers can offer affordable VPN services to the Small and Medium size Business (SMB) and Small Office, Home Office (SOHO) markets. Today, the SMB market represents over 70% of the broadband access market for carriers. This market has not been penetrated by carriers with such value added services as VPN due to the current high entry cost. A self-service version of Secure VCN is available for SMB and SOHO customers. Carriers can bundle this offering with broadband access services such as xDSL, Wi-Fi, GPRS and CDMA2000 1X.

The Secure VCN solution can complement carriers' MPLS-VPN offerings to enterprise customers as well. It enables carriers to attract new enterprise customers, whose requirements cannot be met with MPLS-VPN alone. These include multinational companies, road-warriors and telecommuters anywhere in the world, at a much lower entry point than today's alternatives. Furthermore, with Secure VCN, the carrier service can support all customers' IP applications without exception. Secure VCN services can also meet the requirements of large retailers economically. The following figure depicts the hierarchy of private and secure connectivity services opportunities for carriers.
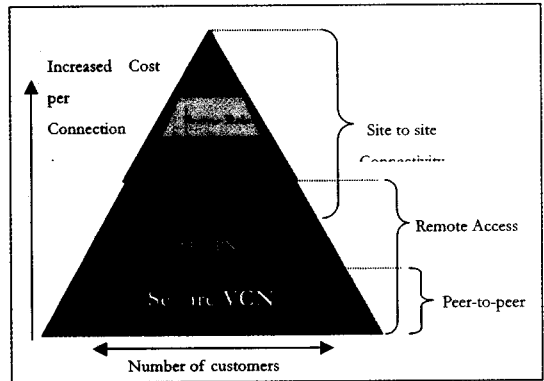
(Figure 2) Carrier Opportunities in Private and Secure Connectivity Services

Short Profile

Dr. Hasan Alkhatib

1975년, 1977년 BS & MS degree in Electrical Engineering from Illinois Institute of Technology and the University of Baghdad.

1983년 Ph.D. in Electrical and Computer Engineering from the University of California

1981년 - 1999년 Director of the Distributed Computing Research Lab and headed the Ph.D. program in Computer Engineering.

1981년- 1999년 Professor of Computer Engineering at Santa ClaraUniversity.

1999 - 현재 President, CEO and Chairman of IP Dynamics, IP Dynamics is the world leader in secure virtual network solutions. Dr. Alkhatib founded IP Dynamics.