VPN White Paper

April 1999

Secure Enterprise Communication

Companies all over the world are changing the way they communicate information, both internally and externally, due to the flexibility and cost-savings of the Internet Platform. Internet Technologies provide secure enterprise-wide connectivity and controlled remote access as well as connection to global resources. They have also created a completely new way to communicate from business to business.

Virtual Private Networking (VPN) is a way to build a secure, private communication infrastructure on top of the Internet. It is a key tool for leveraging the cost savings represented by the Internet in corporate communications. VPNs guarantee privacy and security, allowing companies to communicate information over the Internet inexpensively - regardless how sensitive the data is.

Virtual Private Networking allows companies to communicate with their branch offices, customers, partners, employees, and suppliers effectively and securely. Through VPNs the Internet has become a means of providing more cost effective access to business critical information such as business transactions, order status, inventory levels, or even financial information.

Contents

What is a VPN?

A Virtual Private Network is a private data network that makes use of the public telecommunications infrastructure, maintaining privacy through the use of tunneling protocols and security procedures. VPNs are typically used for linking corporate LANs between sites, company remote workers to the corporate LAN, or external business partners to the corporate network. Furthermore, the public infrastructure in most cases, and specifically for the purposes of this paper, is the Internet

The key VPN technologies include:

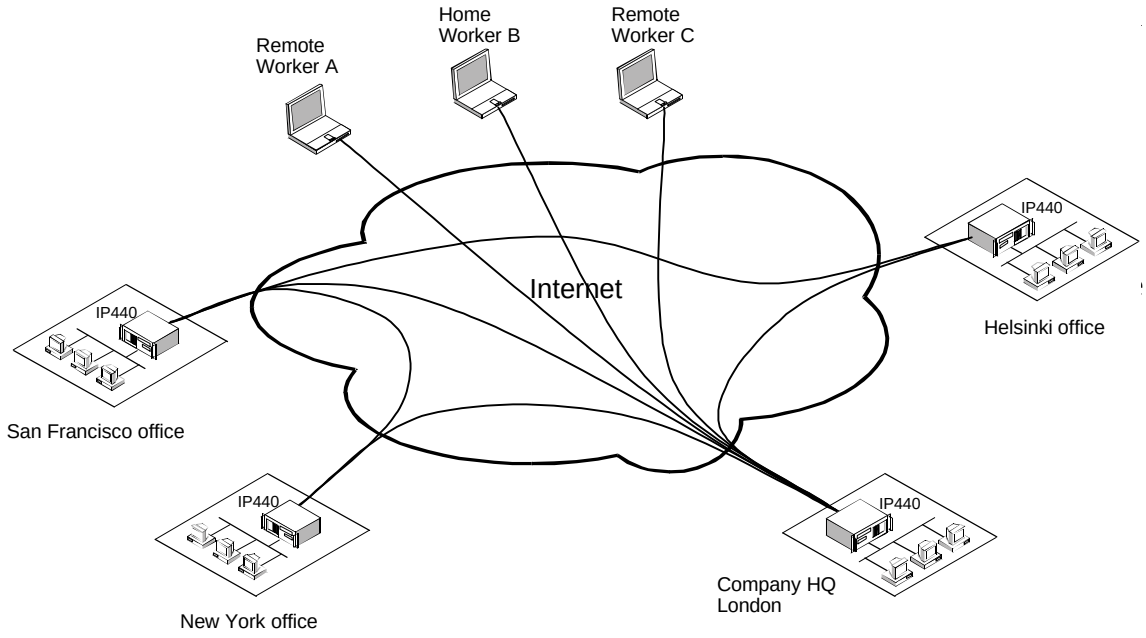

Figure 1: A Virtual Private Network

Figure 1 gives an example of a VPN connecting four geographically dispersed office locations and three individuals working remotely from home or a hotel room.

To implement the VPN in the example in figure 1 you need:

- An Internet access connection (leased line or dial-up) at each location
- Nokia VPN200, IP330, IP440, or IP650 equipment at each office location
- SecureRemote VPN client software on each remote or home worker PC

Once the necessary hardware and software is in place, the network manager sets up the encrypted VPN tunnels between the location from the centralized management system and the network is ready to go. In addition to the VPN capability, you get a secure access to the Internet on each site as a fringe benefit.

The Most Secure Networking Technology

The Internet is exposed to some known security risks. The risks are well known and there are effective solutions available to resolve these security issues. Many other networks and networking technologies are falsely perceived as secure, even though they are mostly exposed to the same security risks as the Internet:

- unauthorized access into internal enterprise networks (break-ins)
- eavesdropping on and tampering with enterprise communications as they pass through the network

The public telephone network is a popular and widely used medium for break-ins. Each modem connected to the public telephone network is a potential break-in point. The security exposure to eavesdropping and data tampering is mainly determined by the accessibility to the cables and equipment carrying the traffic rather than the networking technology, making all networks and networking technologies equally vulnerable.

Virtual Private Networks address these security issues across the Internet, making for the most secure wide area networking solution available.

The Nokia VPN Solution

The Nokia VPN solution provides best-in-class firewall capabilities and highly secure encryption and authentication features. The Nokia VPN solution utilizes encryption to scramble data to ensure that it is practically impossible for a third party to read. Additionally it makes use of data authentication to guarantee the origin and the integrity of the data. No one can falsely act as the other end of the connection or change the content of the packets on the fly. Additional user

authentication is performed to identify the remote users. Access to the corporate network is granted only after a successful, password protected authentication sequence.

The Nokia VPN solution consists of two different product families. The Nokia VPN200 Series appliances provide a cost-effective choice for VPNs where the interface and performance needs are well known. Nokia IP family products (IP330, IP440, IP650) are a more versatile alternative for environments that require better configuration, performance, and routing flexibility. All Nokia security products integrate the proven Nokia networking platform with the market-leading CheckPoint firewall and encryption modules. The Nokia integrated VPN solution secure the communication over the Internet, ensuring the privacy, authenticity, and data integrity.

VPN for Interconnecting Sites

VPNs are ideal for interconnecting Local Area Networks (LAN) between corporate sites. The LAN on a corporate site is connected to the Internet using one of the Nokia integrated VPN gateway products (VPN200 Series, IP330, IP440, IP650). The Nokia VPN gateway encrypts sensitive data communications traveling over the Internet to create a secure tunnel between the sites. There is no need to install and configure encryption software on each host in each network. The gateway performs data encryption on behalf of its encryption domain – the Local Area Network or group of hosts behind the gateway. Data travelling over the public segment of the connection is encrypted, while the communication on the internal network, behind the gateway, is clear text. All of these VPN operations are completely transparent to the end user, and all existing applications are supported.

VPN for Remote Users and Partner Companies

The need to work remotely from home offices or access the corporate network while mobile - from a hotel for example - is growing. Some business partners may also require an access to the corporate network. The Nokia VPN gateway products can be used to extend the enterprise VPN to serve this need. The Nokia IP400 and VPN200 Series products have remote access capabilities built in. The only additional requirement is the Check Point VPN-1 SecuRemote client software on a remote workstation or a laptop using Windows 95/98 or Windows NT. Remote users connect to their corporate networks via Internet using either dial-up or fixed access. The SecuRemote client software establishes a VPN tunnel between the client and the VPN gateway. Once the tunnel has been established, users can transfer sensitive corporate data over the Internet safely and securely, since all communication is protected against eavesdropping and malicious data tampering.

The SecuRemote client encrypts and decrypts data at the network layer enabling it to support all applications transparently. There is no need to change any of the existing applications on the client workstation or laptop. SecuRemote can interface with any existing network adapter or TCP/IP stack and can be connected to several different sites that use VPNs.

Encryption Support

Nokia VPN gateway products support multiple encryption and public key algorithms, as well as several key management protocols, including the support for industry-standard IKE (Internet Key Exchange, also referred to as ISAKMP/Oakley) protocols. Nokia VPN solutions automatically negotiate the strongest possible encryption and data authentication algorithms available between communicating parties. This includes both DES and Triple DES for data encryption and, and SHA-1 and MD5 for data authentication. In addition, encryption keys are updated frequently, ensuring maximum security.

Nokia products provide selective encryption allowing transmission of both encrypted and unencrypted data between two VPN termination points. The network manager simply identifies the specific Internet services and applications, which

are expected to carry sensitive corporate data to be encrypted. Other, less critical information can pass through the network unencrypted. The selective encryption gives the network manager an effective method to optimize the VPN performance.

In large-scale VPN deployments automated key management is necessary to reduce the number of encryption keys to a manageable level. Rather than issuing a unique encryption key for each pair of VPN users, a Public Key Infrastructure (PKI) generates a public key for each individual or application. Whenever someone wants to send an encrypted message to a user, they simply request that user's public key and use it, along with their own private key, to calculate a unique encryption key to secure communications.

Public Key Infrastructure (PKI) relies on digital certificates to exchange public keys. Each certificate carries information about a particular VPN user, including that user's public key, which is used to validate user identity and to calculate the keys for actual encryption. Nokia VPN solutions support open, scalable Public Key Infrastructure utilizing X.509 digital certificates and Certificate Authority (CA) technology from Entrust Technologies. As an Entrust-ready application, the Nokia VPN solution can use Entrust certificates from a trusted CA to initiate secure communications with other IKE-compliant devices.

By supporting Public Key Infrastructure, Nokia solutions enable organizations to automate critical VPN functions, such as adding and deleting users and managing encryption keys.

Flexibility and Cost Savings

VPN's offer incredible flexibility and potentially massive cost savings because of their ability to connect between geographically separated end points by using the Internet. The VPN Research Report , by Infonetics Research, Inc., shows a 20% to 47% savings of wide area network (WAN) costs by replacing leased line infrastructures with VPNs. Remote access VPNs can reduce the corporate remote access dial-up costs by 60% to 80%. On long, international connections the cost savings can be even more dramatic.

These cost savings are achieved by connecting to an Internet Service Provider (ISP) at each network location. Rather than paying for international leased lines between London and

Johannesburg for example, one pay only for a local connection to your ISP at each end of the connection and uses the Internet to connect over the long distance. The same applies for remote access. Instead of making a long distance or international call to a modem pool at the corporate headquarters, a remote user can call to a local ISP and, again, use the Internet for the long distance/international connection.

Internet VPNs extend the coverage and reach of the corporate network. Internet access is available almost worldwide; even in locations where other connection alternatives may not exist.

Using the Internet for connecting corporate sites and remote access users speeds up and allows for more flexibility in network provisioning. All that is needed is an Internet access connection from a local ISP and a Nokia IP400 or VPN200 gateway to add a new site to a corporate network. One interface on the Nokia VPN gateway is connected to the Internet and the other one is connected to the local LAN. A minimal configuration is needed on site to set up the initial connectivity. Once the gateway is reachable via the Internet, the network management center finalizes the security setup remotely. Connecting remote users to the corporate network using remote access VPN is even simpler. First, the network management center configures the user information on the Nokia VPN gateway. Then, SecuRemote client software is installed on the remote user's laptop or a workstation. Once these two simple steps are done, the remote user dials in to the local ISP and is ready to access the corporate network.

Conclusion

The Internet has changed the way companies communicate and disseminate information. Virtual Private Networks are a new way to build secure, private communications infrastructures on top of the Internet. Using VPNs, companies can communicate with their branch offices, customers, partners, employees, and suppliers securely while realizing significant cost savings.

A VPNs is a set of authenticated and encrypted connections on the Internet to connect multiple networks or network devices. They are typically used to connect corporate LANs between sites, remote users to the corporate LAN, or external business partners to the corporate network. The state-of-the-art security technologies make VPNs the most secure networking solution available today.

Nokia VPN gateway products provide a turnkey solution for site-to-site interconnection and remote access applications. They are compliant with the latess security standards and technologies.

Virtual Private Networking is changing the cost of communication as much as the Internet is changing the way corporations communicate. Yet, the administrative overhead of managing complex VPN installations is a recurring cost that the Nokia platform almost entirely mitigates. These cost savings are realized and maintained because of the turnkey nature of the Nokia Security Platform. This series of solutions allows the leveraging the Internet as if it were your own private WAN, without the serious overhead and complexity typically associated with other alternatives.

USA

Nokia
313 Fairchild Drive
Mountain View, CA 94043
+1 650 625-2000

GREAT BRITAIN, NORTHERN EUROPE, EUROPEAN MIDDLE EAST AND AFRICA

Nokia UK Ltd
2 Heathrow Boulevard
284 Bath Road
Heathrow, Middlesex
UB7 0DQ, England
+44 (0) 181 564 3900

ASIA PACIFIC

Nokia Telecommunications
438B Alexandra Road
#07-00 Alexandra Technopark
119968 Singapore

CENTRAL AND EASTERN EUROPE

Nokia Telecommunications
"Merkur-Haus" Hessenring 121
D-61348 Bad Homburg
Germany
+49 6172 925 826

SOUTHERN EUROPE

Nokia Telecommunications
97 Avenue de Verdun
93230 Romainville
France
+33 1 49 15 27 04

LATIN AMERICA AND CARIBBEAN

Nokia
43550 Coal Bed Court
Ashburn, VA 20147
+1 703 236 5030

NOKIA

Visit our Website to find out more about Nokia and Nokia IP Security Solutions

http://www.iprg.nokia.com