Redefining the Virtual Private Network

P/N 31400000101
May 1999

Check Point Software Technologies Ltd.

In this Document:

Introduction	Page 3
Typical VPN Implementations	Page 4
A VPN is More than Just Privacy	Page 7
A VPN Buyer's Guide	Page 7
Check Point's VPN Solution	Page 9
Summary	Page 12

Introduction

The Internet has forever changed the way that we do business. An outgrowth of Internet technology and thinking, Virtual Private Networks are transforming the daily method of doing business faster than any other technology. A Virtual Private Network, or VPN, typically uses the Internet as the transport backbone to establish secure links with business partners, extend communications to regional and isolated offices, and significantly decrease the cost of communications for an increasingly mobile workforce. VPNs serve as private network overlays on public IP network infrastructures such as the Internet.

The effects a VPN can have on an organization are dramatic: sales can be increased, product development can be accelerated, and strategic partnerships can be strengthened in a way never before possible. Prior to the advent of VPNs, the only other options for creating this type of communication were expensive leased lines or frame relay circuits. Internet access is generally local and much less expensive than dedicated Remote Access Server connections.

In fact, according to industry analyst Forrester Research Inc., when comparing the traditional cost of Remote Access Server (RAS) versus today's Internet-based VPN, the cost differences for 1,000 users are significant:

	Traditional RAS Costs	**VPN Costs**
Phone/ISP Charges	$1.08M	$0.54M
User Support	$0.30M	$0.00M (included in user access costs)
Capital Expenses	$0.10M	$0.02M
T1 Lines	$0.02M	$0.03M
Total	**$1.50M**	**$0.59M**
(COSTS PER 1000 USERS)		

Although the electronic information security market is forecasted to grow from $1.1 billion in 1995 to $16.6 billion by the year 2000, sub-markets of this industry, VPNs in particular, are forecasted to grow at even higher rates. According to Infonetics Research, worldwide expenditures on VPNs were $205 million in 1997, and are expected to grow 100% per year through 2001 when they reach $11.9 billion.

Typical VPN Implementations

There are many types of VPN implementations, each with its own specific set of technology requirements. However, VPN deployments can be grouped into three primary categories:

- *Intranet* VPNs between internal corporate departments and branch offices
- *Remote Access* VPNs between a corporate network and remote or mobile employees
- *Extranet* VPNs between a corporation and its strategic partners, customers, and suppliers

In Intranet VPNs that facilitate secure communications between a company's internal departments and its branch offices (see Fig. 1), the primary technology requirements are strong data encryption to protect sensitive information; reliability to ensure the prioritization of mission-critical applications, such as ERP systems, sales and customer database management, and document exchange; and scalable management to accommodate the rapidly growing number of new users, new offices and new applications.

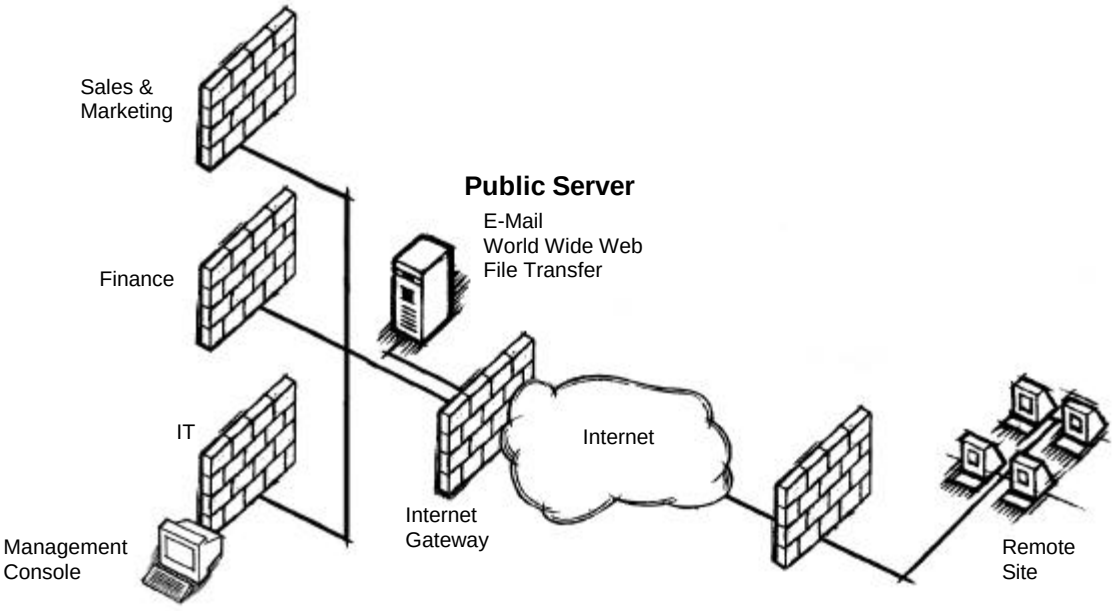

Fig. 1 Intranet VPN

Remote Access VPNs between a corporate network and remote and/or mobile employees (see Fig. 2) have different requirements. Strong authentication is critical to verify remote and mobile users' identities in the most accurate and efficient manner possible. On the management side, Remote Access VPNs require centralized management and a high degree of scalability to handle the vast number of users accessing the VPN.

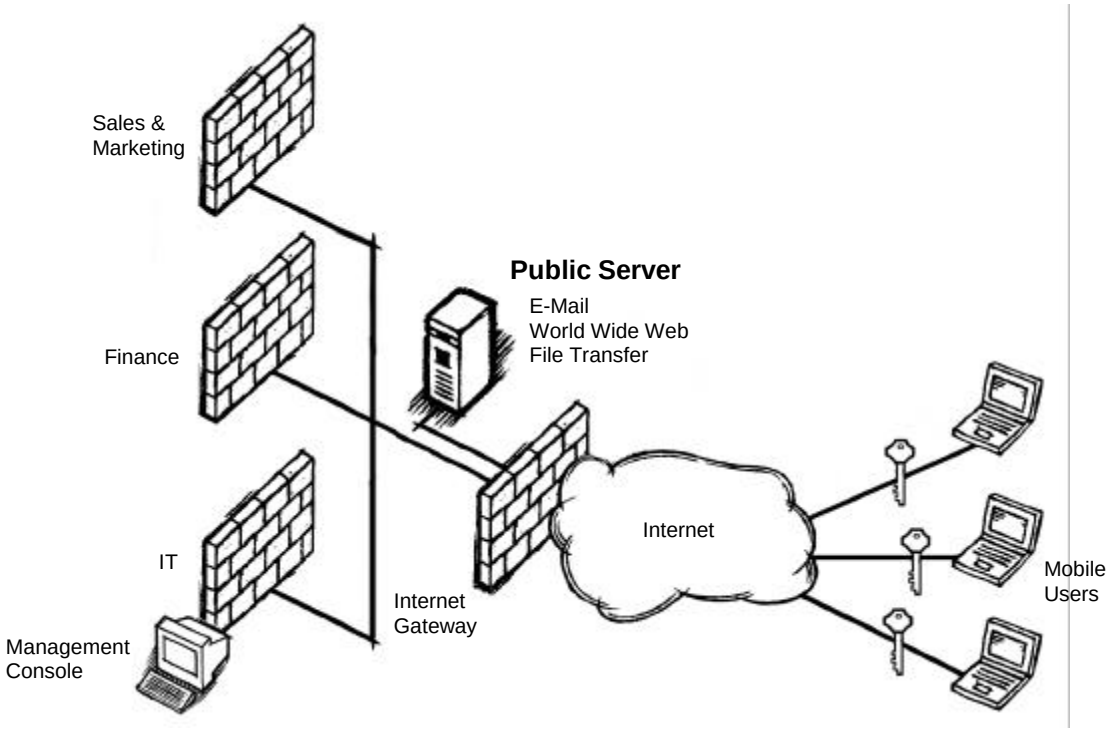

Fig. 2 Remote Access VPN

Finally, Extranet VPNs between a company and its strategic partners, customers and suppliers (see Fig. 3) require an open, standards-based solution to ensure interoperability with the various solutions that the business partners might implement. The accepted standard for Internet-based VPNs is the Internet Protocol Security (IPSec) standard. Equally important is traffic control to eliminate bottlenecks at network access points and guarantee swift delivery of and rapid response times for critical data.

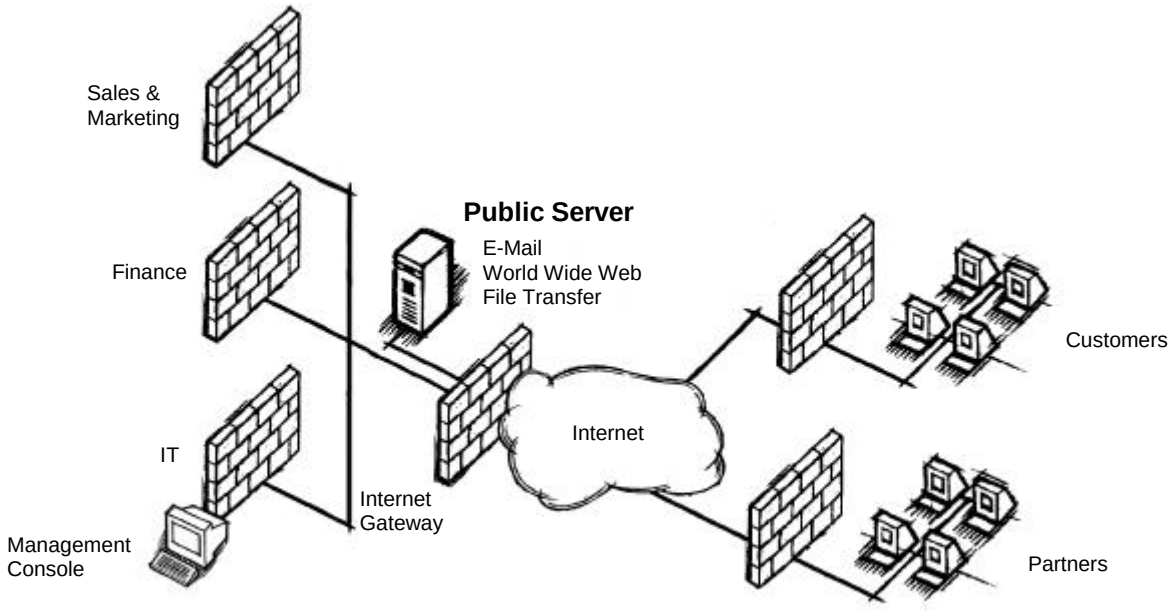

Fig. 3 Extranet VPN

Since VPNs represent only one component in an overall security policy, the challenge is to provide a comprehensive, integrated solution. “One size fits all” just doesn’t apply in the VPN market.

Most VPN vendors today provide solutions tailored to only one of these VPN implementations. This is where the problem lies, since most companies have many remote offices to connect together securely, along with an increasingly mobile workforce, and a desire to leverage the Internet to get closer to customers and business partners. Therefore, a VPN solution must support all three of the above applications, allowing offices worldwide to access network resources, mobile workers to link up to corporate intranets, customers to place orders and suppliers to check inventory levels, all in a highly secure and cost-effective manner. While a corporation may only plan to implement one of the three types of VPNs today, it is imperative that the VPN solution it selects provide the ability to add either or both of the remaining two types seamlessly and easily (see Fig. 4).

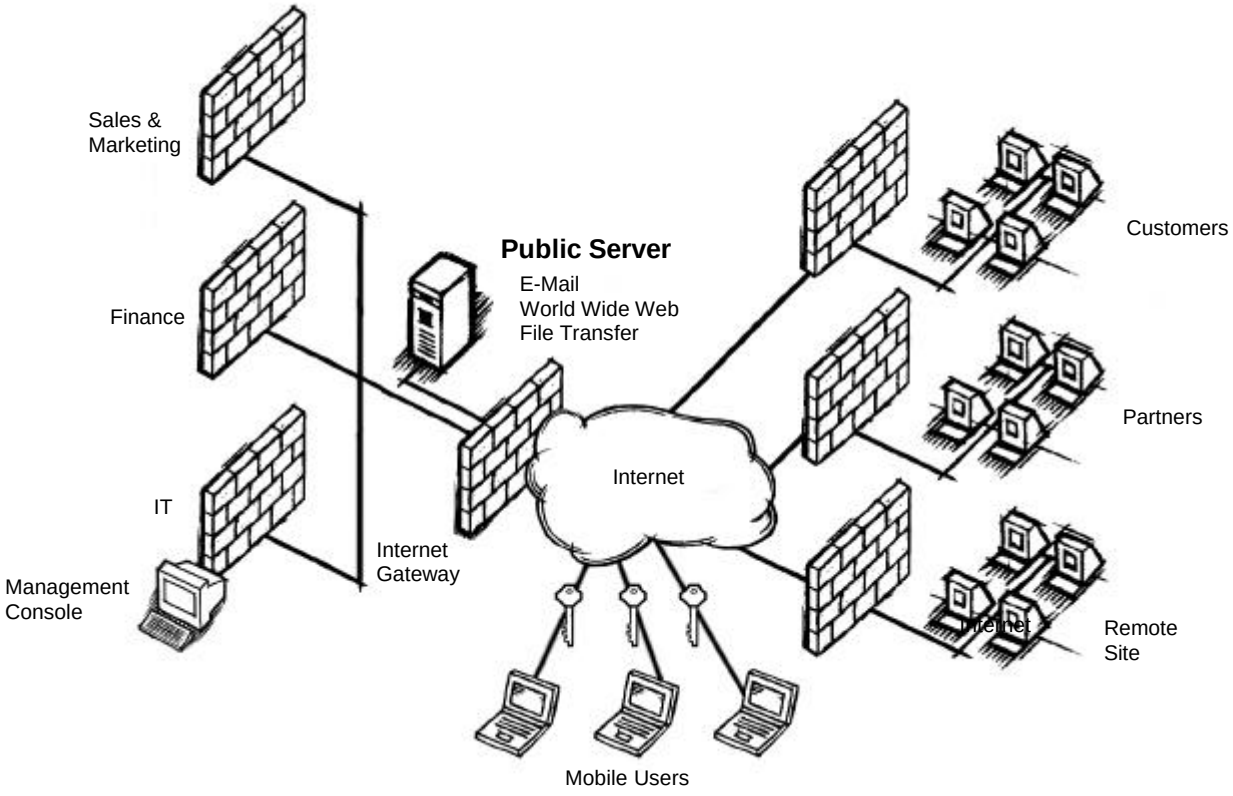

Fig.4 A Complete VPN Implementation for Intranet, Extranet and Remote Access Applications

A VPN is More than Just Privacy

There are a dizzying number of methods for deploying VPNs in today's computing environment. The VPN market is populated with point products and incomplete solutions which focus only on one type of VPN application. Most VPN vendors are offering products that only provide authentication and encryption, leading customers to believe that these two components alone comprise a VPN. However, encryption and authentication alone are inadequate to implement the various types of mission-critical VPNs demanded by companies today.

Standalone VPN products do not usually provide adequate access control. In fact, most vendors sell their VPN products as yet one more networking device which customers must manage separately and somehow integrate into their overall security policy. In addition, most leave the Quality of Service or reliability aspect to the service providers, rather than giving users the tools they need to put performance predictability in their own hands. This piecemeal approach leads to possible security threats, because the VPNs are not integrated into an organization's enterprise security policy, and they provide limited manageability, scalability and interoperability.

A VPN Buyer's Guide

As the worldwide leader in VPN installations, Check Point is redefining what is necessary to create a VPN that goes beyond the "private" in Virtual Private Networking. A VPN is a network that utilizes a public-based infrastructure, such as the Internet, to provide secure, reliable and manageable business-to-business communications. All three of these elements are essential to make a VPN function in today's complex computing environment. This is a radical change in the generally-accepted VPN definition that consists merely of encryption and authentication.

A complete VPN includes the three critical components of:

- Security
  Including access control, authentication and encryption technologies to guarantee the security of network connections, authenticity of users, and privacy and integrity of data communications;
- Traffic Control
  Including bandwidth management, Quality of Service and hardware-based VPN acceleration to guarantee the reliability and performance of the VPN; and,
- Enterprise Management
  Including true policy-based management to guarantee the integration of VPNs within the enterprise security policy, local or remote centralized management of that policy, and scalability of the solution.

"One size fits all" does not apply for VPNs – the combination of these three components is absolutely necessary to enable practical implementation of Virtual Private Networks.

Security

While most VPN vendors provide authentication and encryption, these two technologies only provide privacy for data communications. The security component of a VPN must include all three of the following technologies in order to guarantee the security of network connections, the authenticity of VPN nodes, and the privacy and integrity of data.

Access Control

Access control dictates the amount of freedom a VPN user has, and controls the access of partners, employees and other outside users to applications and different portions of the network. A VPN without access control only protects the security of the data in transit – not the network itself. Rigorous access control capabilities protect the corporation's entire network, including a wealth of intellectual property and information, to ensure that VPN users have full access to the applications and information they need, but nothing more. Both of these key access control capabilities are virtually ignored by most VPN vendors.

Authentication

Authentication is the process of verifying that the sender is actually who he says he is. Support for strong authentication schemes is particularly critical to VPN implementations to ensure the privacy of both gateway-to-gateway and client-to-gateway communications – the identities of both corporate sites and individual users must be verified. A variety of authentication methods are available to meet the needs of particular VPN deployments, including traditional username/password authentication, RADIUS or TACACS/TACACS+ servers, LDAP-compliant directory servers, X.509 digital certificates, and two-factor schemes such as those involving hardware tokens and smart cards.

In addition to the strength of the authentication scheme deployed, other critical factors to consider are broad application support and scalability. Users of any IP-based service must be able to be authenticated in order to establish a secure VPN session. Scalability is of particular concern for remote access VPNs where the number of mobile clients is expected to grow. The authentication scheme implemented for such deployments must be both manageable and easily deployed for large numbers of individual users.

Encryption

Encryption scrambles the data so that only those who have the key to read the information are able to decode the message. Encryption algorithms ensure that it is mathematically impossible to decode the data without possession of the proper encryption key. Generally speaking, the security of the encrypted communication grows as the key becomes longer.

Once the encryption key length is selected and implemented, the next step is to ensure that the keys are protected through a key management system. Key management is the process of distributing the keys, refreshing them at specific intervals and revoking them when necessary. Public Key Infrastructures (PKIs) are essential to VPNs utilizing digital certificates for authentication and encryption, because as VPNs grow in complexity and size, the number of keys to be managed grows accordingly (typically exponentially).

Traffic Control

A natural consequence of increased Internet usage for business communications is network congestion, which can adversely affect the performance of the VPN and other mission-critical applications. As an extension of the enterprise network, a VPN naturally increases network traffic as well as the risk that network performance may be affected. VPN benefits will not be fully realized if users suffer from poor response times, gateway crashes, or other network delays or failures.

A VPN solution must guarantee reliability and Quality of Service by enabling managers to define enterprise-wide traffic management policies that actively allocate bandwidth for inbound and outbound traffic based on relative merit or importance. This ensures the performance of mission-critical and other high-priority applications without “starving out” lower priority applications. The burst and delay effects of Internet traffic are eliminated, allowing network managers to manage or

tune the network traffic using weighted priorities, limits, and service guarantees. This "tuning" approach optimizes network performance and alleviates network congestion for "must see" traffic, forcing less valuable traffic to wait until the most important VPN connections are made. Intelligently managing network bandwidth is one way to ensure that VPN traffic does not slow overall network performance. Today, organizations implementing Virtual Private Networks want a guarantee that the additional processing requirements of the mathematically-based encryption processes will not degrade network performance. The best way to achieve this guarantee is to offload all cryptographic operations to a co-processor dedicated to encrypting and decrypting messages. This not only optimizes performance, it provides an additional measure of safety in the storing of the keys used for the cryptographic functions. Combining both hardware-based acceleration with a software-based VPN solution offers the highest performance, flexibility and scalability possible in today's market, allowing the VPN to scale from T1 links to Fast Ethernet speeds without draining CPU resources.

Enterprise Management

As today's network infrastructure continues to grow, the ability to manage increasing complexity is a crucial differentiator for VPN solutions. A VPN is an extension of the corporation to the outside world, and is therefore also an extension of the enterprise's total security policy. It is imperative that the VPN can be managed from the same integrated console as the rest of the organization's security elements. This is a critical step in implementing a successful and secure network, regardless of the number of regional offices or nodes in the VPN. In addition to ensuring bulletproof security for the organization, centralized, policy-based management offers a number of benefits that translates to swift and easy addition of new users, new offices and new applications, offering the flexibility needed to meet an organization's changing needs.

The rapid adoption of the "extended enterprise" has caused an explosive increase in the number of applications, users, and IP addresses in use across many organizations. Managing this voluminous amount of user information poses formidable challenges for both network and security administrators.

In addition, neither security in general nor VPNs in specific are single-platform applications. Today's networks include a conglomeration of heterogeneous platforms and operating systems. A true enterprise VPN solution must be able work across multiple platforms in order to be effective. In addition to multi-platform support, a VPN must be able to interoperate between different vendors' solutions and applications. For example, a VPN with partners, distributors and customers will likely have implemented a wide variety of security solutions. Interoperability based on industry standards ensures that the VPN will be an effective business communications tool, no matter which vendor's implementation is selected.

Check Point's VPN Solution

In order to effectively utilize the Internet for wide-area communications between enterprise branch offices, mobile workers, and business partners, organizations typically need to implement a combination of intranet, remote access, and extranet VPNs, each with a unique set of security, traffic control, and management requirements. Check Point's VPN-1™ product family addresses all of these requirements in a single, integrated solution. With VPN-1, organizations can integrate a VPN into their overall security framework as easily as adding another rule to the security policy. Once the security policy has been defined, it can be distributed to all network access points and managed from a single, centralized management console.

Security: The First Critical Component

Check Point's VPN-1 solutions integrate access control, authentication and encryption technologies to guarantee the security of the network connections, authenticity of local and remote users, and the privacy and integrity of data communications.

Access Control

Since VPN users may include employees, business partners, customers and suppliers, each with authorization to access only specific information on the network, integrated access control is a key VPN requirement.

Check Point's VPN-1 solutions, based on the industry-leading FireWall-1® enterprise security suite, provide integrated access control with support for over 150 pre-defined applications, services, and protocols out-of-the-box. Once the access control policy is defined, it is automatically deployed to all enforcement points. Check Point VPN-1 eliminates random access security threats and provides the granularity required in a VPN implementation to direct users to only those applications and services which they are authorized to use.

Authentication

Check Point VPN-1 solutions provide integrated support for multiple authentication schemes, providing customers with maximum security and flexibility. Supported user authentication schemes include X.509 digital certificates, two-factor token-based schemes, and the industry-standard RADIUS (Remote Authentication Dial-in User Service) and TACACS/TACACS+ protocols. Check Point VPN-1 also supports integration with LDAP-compliant directories for user-level security information.

Encryption

Once secure network access has been granted, a VPN solution must protect the privacy of the data being transmitted. Check Point VPN-1 meets this requirement by supporting multiple encryption algorithms and encryption schemes, including DES, 3DES, and the IPSec/IKE standards for interoperability. Encryption, decryption, and key management, including support for X.509 digital certificates, are all fully integrated into the Check Point VPN-1 policy-based management system. With VPN-1 solutions, it is even possible to selectively activate encryption on specific services to ensure optimal performance without sacrificing privacy. VPN-1 supports both gateway-to-gateway and client-to-gateway encryption, providing a single solution for all types of VPN deployments – Intranet, Extranet and Remote Access.

The cost savings associated with a large VPN deployment could easily be negated if the VPN solution does not provide an automated key management scheme. PKIs prescribe how keys will be created, delivered and revoked securely for every participating VPN site or node. Since the number of keys increases exponentially with the number of VPN participants, a large-scale VPN implementation quickly becomes impractical without the automated key management performed by PKIs. Check Point VPN-1 solutions provide support for multiple PKIs to ensure interoperability with other third-party VPN applications as well as manageability and scalability for enterprise-wide deployment.

Traffic Control: The Second Critical Component

Before organizations can be confident in utilizing the Internet for business-to-business communications, they must be able to guarantee the reliability and performance of these

communications. For example, the ability to prioritize specific VPN communications, such as business-to-business E-commerce, is a key requirement in this area.

Check Point's VPN-1 solutions meet this requirement with the FloodGate-1™ bandwidth management solution. FloodGate-1 enables customers to define enterprise-wide traffic management policies that actively allocate bandwidth for inbound and outbound traffic based on relative merit or importance to all other managed traffic. FloodGate-1 is the only solution on the market that can manage and prioritize encrypted VPN traffic. By assigning a higher priority to VPN traffic, FloodGate-1 can precisely control the amount of bandwidth for improved VPN reliability and performance. Weighted priorities also ensure that other traffic is not completely starved of bandwidth. FloodGate-1 is integrated with Check Point VPN-1 solutions, sharing the same Stateful Inspection technology for traffic inspection and the same user-defined network objects for easier policy definition. This integration of the security and bandwidth management components is unique to Check Point VPN-1.

Enterprise Management: The Third Critical Component

VPNs represent only one component in an organization's overall security policy. The ability to define a single enterprise-wide security policy that includes VPNs, distribute this policy to multiple enforcement points throughout the network, and manage this policy from a central management console is critical in implementing a secure enterprise network. In addition, the ability to manage increasing complexity and to provide ease of deployment and administration for a growing number of users is a crucial differentiator for VPN solutions.

Check Point VPN-1 solutions uniquely meet these enterprise management requirements. With Check Point VPN-1, VPNs are integrated into the existing enterprise security policy simply by adding another rule. New users, applications and VPN implementations can be added easily via the object-oriented policy editor. Once a policy has been created or modified it is automatically distributed to all network access points. Check Point VPN-1 provides multi-platform support across UNIX and Windows NT servers and internetworking devices from leading hardware infrastructure vendors. Centralized management of all enterprise security components, including VPNs, from a single provides ease of administration both locally and remotely.

Check Point's UAM (User-to-Address Mapping™) technology, a solution within Check Point Meta IP™, further enhances VPN manageability by enabling single sign-on for network resources. The UAM service automatically captures associations between login names, dynamically-assigned IP addresses, and host names, and makes this information available to Check Point VPN-1.

Finally, Check Point VPN-1 solutions provide integrated logging, auditing and reporting capabilities. The graphical log-viewing engine provides the ability to track and consolidate every communication attempt and valid connection. Detailed accounting information can be collected on all communications or on a per rule basis, for greater processing efficiency. Log file data is readily exportable to third-party reporting applications or trouble-ticketing systems. And log information is always authenticated and encrypted to ensure the security of sensitive auditing information.

Summary

A VPN can provide tremendous flexibility and cost savings as corporations extend their network to include remote employees, business partners and customers. However, the benefits of flexibility and cost reductions may be negated if the solution selected is lacking in any one of the critical areas outlined above. With an integrated VPN solution that combines security, traffic control and enterprise management, such as Check Point's VPN-1, companies can realize the benefits of secure, reliable and manageable business communications.

Check Point VPN-1 solutions are comprised of the following products:

- VPN-1 Gateway™
  A tightly integrated software solution comprised of Check Point's market-leading FireWall-1 enterprise security suite and advanced VPN technology.

- VPN-1 Appliance™
  A complete hardware and software security solution providing secure Internet access for branch office deployments.

- VPN-1 SecuRemote™
  Client-side encryption software which extends the enterprise VPN to desktop, remote and mobile users.

- VPN-1 Certificate Manager™
  A complete turnkey PKI solution for Check Point VPN-1 solutions integrating best-of-breed certificate authority and LDAP directory server technologies.

- VPN-1 Accelerator Card™
  A plug-and-play hardware PCI card for Sun Solaris and Windows NT platforms which speeds VPN performance through acceleration of strong data encryption algorithms.

- FloodGate-1™
  A bandwidth management solution that intelligently manages finite bandwidth resources to ensure reliable VPN performance for business-critical applications.

- Meta IP™
  An automated solution for managing IP addressing and naming to ensure control and reliability of address allocation while improving TCP/IP management efficiency.