

CHECK POINT™
Software Technologies Ltd.



We Secure the Internet.

Secure Virtual Network Architecture

A Customer-focused White Paper

P/N 500327
November 2000
www.checkpoint.com

In this Document:

The Evolution of Internet Security	Page 1
Secure Virtual Network Architecture – An Introduction	Page 2
Securing eBusiness Applications – An Emerging Requirement	Page 3
SVN – Securing Networks, Systems, Applications, and Users	Page 3
Key Requirements for a Secure Virtual Network	Page 5
Conclusion	Page 8

© 2000 Check Point Software Technologies Ltd. All rights reserved.

Check Point, the Check Point logo, FireWall-1, FireWall-1 SecureServer, FloodGate-1, INSPECT, IQ Engine, MetaInfo, Meta IP, MultiGate, Open Security Extension, OPSEC, Provider-1, SecureKnowledge, SVN, UAM, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Appliance, VPN-1 Certificate Manager, VPN-1 Gateway, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, and ConnectControl are trademarks, service marks, or registered trademarks of Check Point Software Technologies Ltd. or its affiliates. All other product names mentioned herein are trademarks or registered trademarks of their respective owners.

The products described in this document are protected by U.S. Patent No. 5,606,668 and 5,835,726 and may be protected by other U.S. Patents, foreign patents, or pending applications.

The Evolution of Internet Security

It is indisputable that Internet technology is driving a genuine business revolution. The Internet provides worldwide connectivity and unparalleled cost efficiency, enabling corporations to dramatically transform the way they conduct business. Large numbers of companies, across all industries, are embracing the Internet to expand and re-engineer their traditional business models. The power and openness of the Internet, however, must be balanced with the need to protect the privacy and integrity of information assets.

Not long ago, many network managers believed that simply installing a firewall at their Internet gateway delivered adequate security for the corporate network. But today, the Internet extends deep into many corporations, blurring the line between private and public networks. As the Internet touches more elements of the network, the corporation's security deployment must keep pace in order to guarantee the protection of all network resources and business communications.

Just as importantly, the security implementation must not impair the openness and accessibility of the network. Any strategy that relies upon limiting access to services, users and network resources to achieve security is doomed to fail. The Internet will continue to push the boundaries of the corporate network and require a comprehensive Internet security strategy to support today's eBusinesses. To meet the dual, and often conflicting, demands of providing both security and openness Internet security must be an integral component of any enterprise network or eBusiness strategy.

Additionally, an effective Internet security strategy must also account for emerging threats. Foremost among these are threats originating from inside the corporate network, as well as those created by the remote access of corporate network resources. It is well known that the majority of network security breaches come from within the corporation. These often involve independent contractors on the LAN, or disgruntled or curious, network-savvy employees with access to sensitive business applications or databases. A robust Internet security deployment must protect against all threats, regardless of origin.

Remote access to network resources poses another set of challenges. Connecting a remote user to the corporate network via an Internet-based virtual private network (VPN) effectively extends the network's security perimeter to that individual's laptop or desktop machine. To maintain the integrity of the security infrastructure the remote user's machine must remain secure at all times so that it cannot be used to infiltrate the company's network using an authorized VPN connection.

To successfully meet all of these Internet security challenges requires a comprehensive architecture that can connect and secure all elements of an eBusiness: networks, systems, applications and users. Managing end-to-end security requires a scalable, policy-based solution that can protect all Internet, intranet and extranet communications. This is what a Secure Virtual Network is all about.

Secure Virtual Network Architecture – An Introduction

Check Point's Secure Virtual Network (SVN) is a true security architecture that provides an integrated framework for deploying and managing an Internet security implementation. SVN is comprehensive in its approach to securing a corporation's network. It integrates multiple capabilities, including firewall security, VPNs, IP address management and more - all within a common management framework. This tight product and management integration enables a security manager to define and enforce a single policy that incorporates all aspects of network security.

No.	Source	Destination	Service	Action	Track	Install On
1	Sales@Any	Local_VPN_Domain	Any	Client Encrypt	Long	Gateways
2	Remote_VPN_Domain	Local_VPN_Domain	Any	Encrypt	Long	Gateways
3	Any	Email_Server	smtp	accept	Long	Gateways
4	Email_Server	Any	smtp	accept	Long	Gateways
5	Local_Net	Any	Any	accept	Long	Gateways
6	DMZ_net	Local_Net Remote_Net	Any	reject	Alert	Gateways

Figure 1: VPN-1/FireWall-1/FloodGate-1 rule base

The SVN architecture eliminates the need to deploy a patchwork security solution comprised of multiple, non-integrated products. Based on a common management foundation, SVN solutions provide unparalleled security, while maintaining an open and accessible network environment. It was designed from the ground up to meet the security, reliability and manageability requirements of demanding eBusiness environments.

Security policies managed within the SVN architecture can be defined centrally and distributed to multiple enforcement points for end-to-end Internet security. Automatic distribution of an enterprise-wide security policy guarantees consistent enforcement and is the only answer to providing scalable security management.

A Secure Virtual Network establishes the model by which organizations can leverage the Internet to connect all elements of a corporate network, but deliver the security and reliability typically expected only with private networks. An SVN is much more than a firewall deployment or a VPN installation. It provides a completely integrated approach to Internet security that enables organizations to gain the cost and connectivity benefits of the Internet, without compromising performance or the integrity of the corporate security policy. It delivers a level of security and manageability that cannot be attained by deploying non-integrated, discrete products (e.g. separate firewall and VPN deployments).

Securing eBusiness Applications – An Emerging Requirement

Before any organization is able to fully capture the benefits of an eBusiness model they must deploy a robust security infrastructure. Today, many companies have heterogeneous application environments that lack basic security functionality. For example, without the ability to accurately identify users and provide the proper level of authorization, the applications driving eBusinesses may likely be exposed to serious security threats. Not only do very few applications incorporate strong security, but also most cannot be easily modified to incorporate these important capabilities.

A Secure Virtual Network protects not only the network and business communications, but can be extended to secure the application environment. Integrating the security infrastructure with the application environment provides full security for the eBusiness, while allowing organizations to easily establish and maintain trusted relationships with third-party organizations and individuals. SVN delivers a common security layer that authenticates users to eBusiness applications. Organizations deploying multiple eBusiness applications can leverage a comprehensive security architecture to capture important information about users, thus enabling the applications to make the correct authorization decision. With SVN, security is no longer an impediment to the rollout of a broad eBusiness initiative.

SVN – Securing Networks, Systems, Applications and Users

Check Point's SVN architecture is designed to meet the challenges of eBusiness and connect the four elements common to any enterprise network: networks, systems, applications and users.

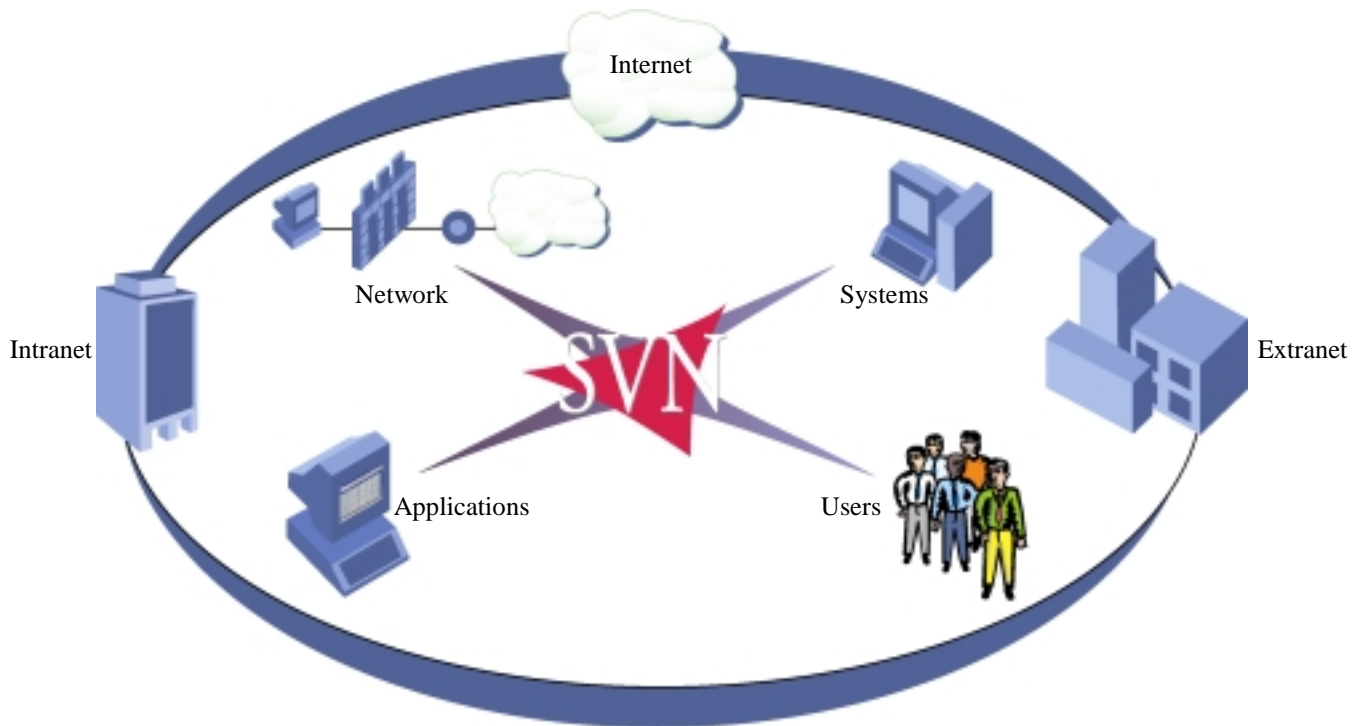


Figure 2: SVN Diagram

The following section provides a detailed discussion of the security requirements for each. Security managers and IT professionals should only consider Internet security solutions that successfully address all of these components.

Networks

A network security strategy must protect all networks within the corporation and support a variety of access technologies. This includes local area and wide area networks, as well as networks connecting using broadband and wireless technologies. It is important to realize that any network left unprotected can jeopardize the security of the entire organization.

A secure network also depends on having the right network management infrastructure in place. Security is irrelevant if users don't have basic network connectivity allowing them to access resources and information. To do this requires efficient management of an organization's IP address and name space, which rely on network services such as the Dynamic Host Configuration Protocol (DHCP) and the Domain Name Service (DNS). Efficient and centralized management of IP addresses builds the foundation for a Secure Virtual Network.

Even with bulletproof security, users and applications must receive the necessary performance to maximize the usefulness of the network. It is counterproductive to secure the network while degrading performance such that users can't access data and applications reliably. Delivering the right quality of service (QoS) is imperative to maintaining the performance and utility of the enterprise network. Integrating quality of service capability, such as bandwidth management, enables a single policy to provide both security and performance.

Systems

To deliver effective Internet security, network managers must protect all systems within the organization. This includes servers, desktop PCs, remote clients, cell phones, personal digital assistants (PDAs), and any other device used to access the corporate network or the Internet. The security solution must not only protect the device from attack, but also secure communications between that system and the corporate network.

Protecting internal servers against internal attacks highlights the need to protect critical systems throughout the organization. Although a corporate firewall remains a core component in protecting the network, it cannot guard against malicious internal users who are targeting local resources for attack. Security managers should deploy network-level security for sensitive application servers. For example, this means running a firewall on an internal SAP accounting server to prevent personnel outside the finance department from accessing sensitive accounting data.

Desktop PCs can also contain sensitive data that requires the attention of the security manager. Personal firewall software may be required to protect individual hosts throughout the network. As with firewall software protecting individual servers, personal firewalls should have their policies defined and managed centrally for consistent security enforcement.

In addition to protecting against network intrusion, a reliable security deployment must protect itself against attack. One of the more common attacks lodged against security gateways and servers is denial of service attacks. Rather than attempting to penetrate network defenses, denial of service attacks attempt to render Web servers or complete networks inaccessible to legitimate users. The attacks are carried out by flooding the network with very large numbers of requests with the intent of consuming computing resources and shutting down service. An Internet security solution must provide the means to detect and respond to denial of service attacks and protect the availability of resources.

Applications

Internet security installations must support a broad range of applications, including those delivering eBusiness, E-Commerce and multimedia services. Securing these services requires the application-level awareness and high performance of Stateful Inspection. Application awareness ensures that authorized network services are not being misused for nefarious purposes.

For example, how does one guarantee that what appears to be HTTP traffic (TCP port 80) is not actually some other service using this authorized network port to plant a Trojan horse in the network. Rudimentary packet filtering products are susceptible to these simple attacks and should never be relied upon for network security. Only technologies like Stateful Inspection secure a broad range of applications and ensure the integrity of traffic being allowed into the network.

Users

Often the focus of network security is how to secure internal resources against external threats. However, when making the corporate network accessible to users via remote access VPNs the security policy must guarantee that unauthorized individuals do not gain access to confidential data. For instance, many organizations may want to make customer data available to a sales manager via the corporate VPN, but block access to all other users.

To deliver this level of granularity, the security policy must support user-based access control and enable mechanisms by which users can be authenticated prior to being granted network access. There are numerous user authentication methods and products delivering a range of authentication strength and ease of use. For most remote access deployments it is recommended to use a strong, two-factor authentication technique, such as smart cards, one-time passwords, or digital certificates, which can be stored securely in a hardware or software token. Strong user-based authentication ensures that only the right users get access to specified data.

Organizations can enhance their network security by enforcing user-based access control for internal clients wishing to access the Internet. To avoid repeated authentication challenges, which can make the network much less user friendly, organizations should look to leverage existing user authentication data. For example, users are typically forced to authenticate to the network before gaining network privileges. An intelligent security deployment can leverage this authentication information in the enforcement of network security so internal users are not challenged each time they access either internal or external resources.

Key Requirements for a Secure Virtual Network

There are many dimensions upon which an Internet security solution can be evaluated. Too often, security managers make purchase decisions based on one or two important criteria, but fail to consider other important aspects of the deployment. A security installation that fails to meet a comprehensive list of requirements is destined to fail.

To realize the benefits of a Secure Virtual Network requires satisfying five key requirements.

- Security and Management
- Performance and Scalability
- High Availability
- Interoperability
- Comprehensive

Security and Management

The need to provide secure and manageable Internet security appears obvious on first examination. However, there are important requirements that must be met to deploy a Secure Virtual Network architecture that can be efficiently managed.

- *Integrated policy-based management* - Integrating all components of Internet security (firewalls, VPNs, content security, QoS, address translation, and more) into a single policy. Replacing a multitude of non-integrated management tools with a single security policy enables greater management efficiency.
- *Centralized management with distributed deployment* – Automatically distributing security policies throughout the enterprise to guarantee consistent enforcement. The expansion of a corporate network, as measured by an increasing number of Internet access points or users, should not place an additional management burden on security administrators. Truly centralized management enables the automatic deployment of a single policy to multiple security gateways or users.
- *Application and user-based policies* – Delivering granular access control to network resources based on service or authenticated user information. Security policies must have the intelligence to enforce security based on specific applications or users, and should never rely solely on information contained in IP packet headers, as is done with simple packet filtering firewalls.

Performance and Scalability

For an Internet security deployment to remain viable in rapidly growing eBusiness environments it must scale to meet increasing network demands. In addition, it must never degrade the performance of the network infrastructure. To the greatest extent feasible, Internet security should remain transparent to the user community.

When evaluating the performance and scalability of Internet security solutions, the following parameters must be fully considered.

- *Support for highest throughput and concurrent users* – Supporting high data throughput rates (multiple T1s, T3/E3 links, and higher) and large numbers of simultaneous users. A Secure Virtual Network architecture must provide support for technologies that enable organizations to meet increasingly higher performance targets. This includes Stateful Inspection-based security, hardware-based VPN acceleration and Internet gateway clustering.
- *Integrated bandwidth management* – Integrating bandwidth management with Internet security to deliver reliable Quality of Service (QoS) for all Internet, intranet and extranet traffic. Only when bandwidth management is fully integrated with security enforcement can an organization deliver traffic prioritization that is consistent with the corporation's business objectives. For example, most eBusinesses will grant a higher bandwidth priority for E-Commerce traffic supporting on-line purchasing than inbound email traffic, which is typically time insensitive.
- *Scalability for enterprise-wide deployments* – Scaling the Internet security infrastructure to support dispersed networking environments. Organizations require security throughout the organization, not just at Internet access points. Security enforcement extends to application servers, departmental networks, desktop users and telecommuters. A Secure Virtual Network requires an effective and scalable means to manage security across the entire corporation on a variety of platforms and operating systems.

High Availability

With eBusinesses completely dependent on the Internet, organizations must build their Internet Security infrastructure to deliver high availability (HA) so that single points of failure are eliminated. By providing high availability, a Secure Virtual Network will guarantee that the network is always available to support critical applications and users. Among the many HA requirements include:

- *Transparent fail over without loss of connectivity* – Keeping Internet connections intact and unaffected by a single failure in the security infrastructure. As an example, if an Internet gateway supporting firewall or VPN services were to fail, existing connections should be seamlessly supported by a backup gateway.
- *Resilient remote access VPN support* – Providing remote VPN users with access to internal network resources via multiple Internet gateways. Enabling a telecommuter to connect with one of several alternate VPN gateways if the primary gateway is unavailable delivers a resilient VPN solution – and provides a superb level of high availability.
- *Load balancing* – Leveraging multiple Internet Security gateways to provide improved aggregate performance through clustering. When one or more VPN/Firewall gateways is used to protect and provide connectivity to a network, load balancing can be used to distribute the traffic load among several machines. The result is performance that cannot be matched by simply moving the security enforcement to a higher end platform.

Interoperability

Successful Internet security deployments must be based on an open platform and adhere to a broad range of industry standards. Security products built using proprietary technology without any support for multi-vendor interoperability will not scale to meet the demands of a Secure Virtual Network. Interoperability must be met on a number of fronts:

- *Open Platform for Security (OPSEC)* – Delivering best of breed Internet security through support for open application programming interfaces (APIs). As a complete policy management framework, OPSEC provides the central integration, configuration and management of third-party products and services that is required by a Secure Virtual Network Architecture. OPSEC support ensures that an Internet security deployment is always extensible in order to incorporate the latest technological advancements in security and policy management.
- *Industry standards* – Supporting industry-standard protocols, algorithms and interfaces to guarantee multi-vendor interoperability. Secure Virtual Networks use Internet technology to securely connect corporations to business partners and customers. To enable reliable communications, solutions must adhere to industry standards such as IPSec (for VPNs), LDAP (for directory-based user management) and many others.
- *Open PKI and multiple authentication* – Establishing secure VPN communications and granting authorized network access using flexible authentication methods. Authenticating network users before granting access to sensitive network resources is a critical requirement of a Secure Virtual Network architecture. An SVN solution must support a broad range of authentication technologies and products, including tokens, one-time passwords, biometrics and others. Increasing adoption of public key infrastructures (PKIs) for authentication and VPN key management requires support for X.509 digital certificates generated by multiple CA vendor products.

Comprehensiveness

- *Internet, intranet and extranets* – Extending security to all communications across a spectrum of networks. An effective and reliable Secure Virtual Network relies on comprehensive coverage of all communications, including Internet, intranet and extranet traffic. Ignoring just one class of traffic can expose the larger enterprise network to unacceptable security threats.
- *Gateways, clients, and servers* – Deploying security throughout the organization for complete protection. A Secure Virtual Network requires a multi-layered approach to security that enforces enterprise policies on Internet gateways, individual desktops, applications servers, remote users and others.
- *Multiple platform support* – Enabling security in heterogeneous networking environments. Complete network protection with the SVN architecture demands that security be deployed and enforced on a large number of network platforms, devices and operating systems. Comprehensiveness is achieved by providing full Internet security for platforms as diverse as appliances, Windows operating systems, Unix servers, switches and others.

Conclusion

A Secure Virtual Network architecture provides a scalable, integrated framework for deploying and managing Internet security. It is designed to meet the security requirements for today's eBusiness and provide a solid foundation for emerging security needs. SVN establishes the model by which organizations can leverage the Internet to connect and secure all elements of the network.

About Check Point Software

Check Point Software Technologies offers a full range of solutions that solve the networking challenges you're facing today. As the worldwide leader in securing the Internet with its Secure Virtual Network (SVN) architecture, Check Point has helped over 47,000 customers with over 125,000 installations solve their network security challenges. In the area of Virtual Private Networks (VPNs), Check Point has connected over 42,000 VPN gateways and millions of mobile and remote users.

With the broadest range of products built upon Check Point's SVN architecture, our experience in providing comprehensive solutions to your organization's networking needs is unmatched. Whether you are setting up a Web server or E-Commerce site for the first time, striving to lower your company's remote access costs, or planning to extend your enterprise to include strategic partners, Check Point has worked with thousands of companies to identify and solve the most critical network security challenges.

About Check Point Software

Check Point Software Technologies offers a full range of solutions that solve the networking challenges you're facing today. As the worldwide leader in securing the Internet with its Secure Virtual Network (SVN) architecture, Check Point has helped over 47,000 customers with over 125,000 installations solve their network security challenges. In the area of Virtual Private Networks (VPNs), Check Point has connected over 42,000 VPN gateways and millions of mobile and remote users.

With the broadest range of products built upon Check Point's SVN architecture, our experience in providing comprehensive solutions to your organization's networking needs is unmatched. Whether you are setting up a Web server or E-Commerce site for the first time, striving to lower your company's remote access costs, or planning to extend your enterprise to include strategic partners, Check Point has worked with thousands of companies to identify and solve the most critical network security challenges

Check Point Offices

International Headquarters:
3A Jabotinsky Street, 24th Floor
Ramat Gan 52520, Israel
Tel: 972-3-753 4555
Fax: 972-3-575 9256

e-mail: info@Checkpoint.com

U.S. Headquarters:
Three Lagoon Drive, Suite 400
Redwood City, CA 94065
Tel: 800-429-4391 ; (650) 628-2000
Fax: (650) 654-4233

URL: <http://www.checkpoint.com>