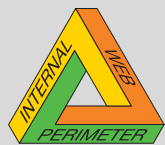


Achieving Network and Application Protection: How Network-Based Solutions Mitigate Risk for Internet Data Center Environments

In this Document

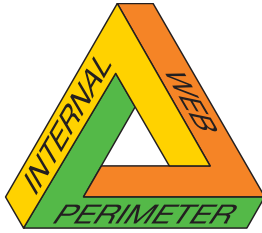
- 1 Executive Summary
- 2 How Network-Based Solutions Mitigate Risk for Internet Data Center Environments
- 3 The Challenge
- 4 The Check Point Solution
- 5 Scenarios
- 6 Delivering Network and Application-Level Protection with SmartDefense
- 7 Achieving Centralized Management with SmartCenter and Provider-1
- 8 Conclusion



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Executive Summary



Intelligent Security

Service providers and enterprises are under constant pressure to reduce the cost of securing complex environments such as data centers, points-of-presence (POPs) or large, segmented corporate networks. Virtual LAN (VLAN) technology is often used to simplify the network topology in these environments and a common practice is to place a dedicated firewall or VPN device in front of each network segment.

However, deploying and maintaining large numbers of these dedicated devices can be expensive and time consuming because

Internet Data Centers (IDCs) and service provider POPs can be complex network environments. As a result, enterprises and service providers are always looking for ways to manage their data center and infrastructure environment with greater efficiency and agility.

To achieve these goals, service providers and enterprises require solutions that unify management architecture for POP and Customer Premise-based Equipment to suit small, medium and enterprise segments. With a unified management architecture, service providers and enterprises can lower total cost of ownership for management and use Data Center manpower more efficiently. Also, since they will be using rack space more efficiently, they will lower costs associated with labor and rent.

Beyond the value derived from a reduction in capital investment, a lowering of administrative overhead costs, and the simplification of policy provisioning, customer demands for more sophisticated services requires an integrated solution that delivers access control, remote access and attack protection from a single solution. Network-based solutions meet these basic requirements and enable service providers and enterprises to leverage their existing security infrastructure.

Being able to aggregate multiple security policies on a single platform is valued because it decreases management overhead, lowers hardware investment and reduces data center space requirements while accelerating security deployment. An intelligent security solution specifically designed for VLAN-enabled environments — from data centers and POPs to large, segmented networks — is needed to address trends in the industry that are combining to make network and application protection an essential part of running any mid-sized or large business.

The rising costs associated with internal security breaches and external attacks and the increasingly decentralized workforce that has created over 2 million remote offices in the United States alone will combine to force organizations to resolve information security issues across the entire enterprise and will require service providers to adapt to evolving market conditions. Although the threat of security breaches and the trend toward workforce decentralization have deeply concerned information security experts for a number of years, increasing government regulation has helped to make the deployment and management of network security into a business-critical problem that companies are legally obligated to resolve.

Security Breaches

In 2002, Computer Economics Inc. estimated that hackers, worms, and other high-tech intrusions caused approximately \$11.1 billion in damages. In an article published by Reuters on January 19, 2004 it was estimated that computer virus attacks cost businesses around the world approximately \$55 billion in damages in 2003. This amount is expected to increase this year. According to analysts, the number of attacks between January and June 2003 exceeded 70,000. This is approximately twice the rate for 2002.



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

Workforce Decentralization

The decentralization that results from globalization, the cutbacks in office space in order to decrease overhead and the popularity of flexible work hours has created a shift away from a centralized corporate office and encouraged an increasingly large portion of the labor force to work in home offices or small offices that don't have dedicated IT staffs. According to In-Stat/MDR, 58% of US employees already work in locations outside of their corporate headquarters. As a result, backing up and protecting remote office data is becoming increasingly difficult for IT managers and corporate officers, who are now legally responsible for a company's compliance with recent regulations

Regulatory Compliance

According to a December 30, 2003 article in Computerworld, remote offices are the "Achilles' heel of regulatory compliance." Even though companies have spent millions of dollars each year to ensure compliance with the Sarbanes-Oxley Act, HIPAA, USA Patriot Act, EU Data Protection Directive, Common Criteria, or the recent California Data Security Act and others, most companies fail to properly secure their networks and data despite the possibility that auditors can levy steep fines and corporate executives can face jail time.

The decentralization of the corporate workplace, the excessive losses incurred as the result of internal and external attacks, and the increasingly stringent regulations relating to information security will motivate corporations to seek solutions that provide centralized network and application protection that seamlessly integrates within an existing IT infrastructure.

How Network-Based Solutions Mitigate Risk for Internet Data Center Environments

Current VPN Deployment Trends

A popular solution for an organization's Internet connectivity needs is a virtual private network (VPN). A VPN is a private network that is configured and operates within a public network. To establish this private network data integrity and confidentiality are protected through authentication and encryption. For example, data can be securely transmitted between two branch locations across the Internet or be encrypted between a server and a client within a Local Area Network (LAN). An In-Stat/MDR survey of enterprise users in 2003, found that 89% of respondents were either currently using a VPN or planned to use a VPN within the next two years.

Customers are increasingly comfortable with having their service provider either remotely manage their Customer Premise-based Equipment (CPE) or host their network-based solution. The In-Stat/MDR survey in 2003, indicates that 72% of those who currently use VPNs would consider outsourcing to a service provider. According to the survey, the main drivers are the need to reduce ongoing operating costs, decrease IT headcount and combine multiple networks.

Even though there are many financial and functional benefits to utilizing a provider-managed VPN solution, achieving end-to-end security has been a challenge. Customer Premise Equipment (CPE) solutions inherently offer end-to-end encryption of data traffic, but this is not typically the case with network-hosted solutions. Until now, organizations taking advantage of network-hosted solutions needed to invest extensively in hardware and personnel in order to achieve end-to-end security. With Check Point's full range of solutions, organizations can now run up to 250 virtual firewalls on a single, extensible hardware platform. By eliminating the need to deploy multiple hardware platforms, Check Point delivers integrated end-to-end protection against dynamic Internet threats that enables organizations to reduce their hardware investment, decrease data center space requirements, accelerate security deployment and lower management overhead.



Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

The Challenge

Corporations and service providers, under increasing pressure to reduce the cost of securing high-speed, mission-critical environments like data centers, POPs and large, segmented networks, have embraced network-based solutions to simplify these complex networks. Unfortunately, it has been difficult to secure this network architecture efficiently. Traditionally, most organizations deploy separate firewall, VPN and attack protection devices in front of each network segment or even each server, but many organizations and service providers are searching for more efficient solutions to maintain these networks more effectively.

Given the internal and external threats to data security, the difficulties associated with attempting to integrate diverse technologies and vendors, the fact that some departments need to be protected from each other, and regulation compliance issues, creating data security across an enterprise's network has never been more important, but organizations continue to address data security in a piecemeal fashion because some executives don't understand that the entire security architecture is interdependent. Often, a company will only focus on their perimeter defenses or their web security. These companies can not achieve worry-free protection without protecting their perimeter, internal and web security. If any one segment of the security architecture remains vulnerable to attack, the entire network is at risk. Other organizations have tried to cobble together a secure architecture using different products and vendors. For the most part, this has been a frustrating experience because it is often difficult to manage and maintain disparate product vendors, specialized security experts, access providers and systems integrators. For this reason, taking an integrated network and application approach to information security is the best defense against the next generation of threats.

As a result, enterprises and service providers are increasingly interested in products and services like Check Point's Application Intelligence™ (AI) that offers stronger security for more protocols, thorough application-level inspection and adaptive protection for defending against all current and emerging threats. Given the increasingly sophisticated attacks that are well past scanning for open ports on firewalls and now directly attack applications, an organization's information security needs to provide comprehensive security on multiple levels. These levels of security should protect against both network and application attacks, while providing robust access control to IT resources.

Many organizations today rely on multiple management interfaces and this makes it difficult to ensure that the security policy is always up-to-date at all enforcement points. Organizations need to take advantage of centralized management solutions like Check Point's Smart Management Architecture (SMART) solutions that combine VPN, firewall, Network Address Translation (NAT), personal firewall and Quality of Service (QoS) policy editors into a single integrated application that strengthens an organization's security.

To win the trust of customers, a provider must be able to deliver a single solution that offers access control, remote access, and attack protection that will reduce capital investment, and reduce administration overhead as well as simplify security policy provisioning. The provider must also integrate with the existing security infrastructure, accommodate widespread platform support, offer consistent high performance without compromising network performance, use proven security technology, and provide value added services like reporting, security scanning, virus scanning, and intrusion detection.



Intelligent Security

Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

The Check Point Solution

Ninety-seven of the Fortune 100 relies on our solutions because Check Point offers the most intelligent security, the industry's only fully-integrated and centralized management architecture, the only extensible architecture that can adapt to today's dynamic security threats and a software-based approach that leads to higher performance.

Check Point solutions deliver comprehensive attack protection and network security by using Stateful Inspection technology, invented and patented by Check Point. Stateful Inspection is the de facto standard in network security technology and is founded on INSPECT™ technology. Stateful Inspection architecture utilizes a unique, patented INSPECT Engine, which enforces the security policy on the gateway where it resides. The INSPECT Engine looks at all communication layers and extracts only the relevant data, enabling highly efficient operation and support for a large number of protocols as well as applications and easy extensibility to new applications and services. Stateful Inspection provides accurate and highly efficient traffic inspection with full application-layer awareness for the highest level of security. Customers experience higher performance and scalability as well as the ability to support new and custom applications.

This is augmented with Check Point Application Intelligence (AI). AI is a set of advanced capabilities, integrated into Check Point FireWall-1®, SmartDefense™ and VPN-1® VSX. AI detects and prevents application-level attacks. Also based on INSPECT, AI redefines the network security landscape by evolving FireWall-1 into the only security gateway solution that integrates both network and application-level capabilities to deliver comprehensive attack protection and network security.

Whether an enterprise is using a self-managed CPE-based solution or working in partnership with a service provider to benefit from a provider-managed CPE-based solution, network hosting, or hybrid VPN solution, Check Point offers solutions that provide integrated protection against network and application threats.

When an enterprise or a service provider wants to simplify their network topology, Check Point leverages Virtual LAN (VLAN) technology to deliver a high-speed, multi-policy security solution that is specifically designed for enterprises, data centers, and service provider POPs.

VPN-1 VSX is designed to address the unique and sophisticated requirements of enterprise data centers and service providers. VPN-1 VSX enables multiple networks to be protected, remain connected to shared resources — the Internet and DMZs — and allows networks to interact with each other in a safe, secure environment that allows for a simplified and unified management that increases flexibility and reduces hardware costs.

Enhanced to include Check Point's best-in-class Application Intelligence technology, SmartDefense attack protection, and VPN-1 SecureClient™ remote access and desktop security, VPN-1 VSX equips service providers and enterprises with highly intelligent and integrated end-to-end protection against dynamic Internet threats. This enables them to strengthen their security while taking advantage of the cost efficiencies of a Virtual System (VS).

Virtual Systems execute routing, enforcement and management functions. Virtual Routers eliminate the need to have physical routers by connecting Virtual Systems to shared resources, which can either be trusted, like an organization's LAN, or distrusted, like the Internet. Enforcement Virtual Systems are a completely virtualized version of the standard VPN-1 or FireWall-1 enforcement point and contain their own security policy. In addition, it also provides SmartDefense attack protection capabilities, delivering the highest level of security to the network it protects. Multiple Virtual Systems may be associated with a single physical interface on the gateway using VLAN



Intelligent Security



We Secure the Internet.

technology. This enables customers to easily scale to hundreds of Virtual Systems on a single platform. Each Enforcement Virtual System has its own State Tables, Security and VPN Policy, configuration parameters, separate TCP/IP stacks, and Secure Internal Communications certificate. A Management Virtual System allows you to connect your management server to the VSX gateway and also includes the High Availability (HA) synch interface that enables an organization to deploy VSX in an HA configuration.

Specifically designed for VLAN-enabled environments — data centers, POPs and large, segmented networks — VPN-1 VSX can aggregate up to 250 discrete security policies on a single platform, minimizing hardware investment, delivering Check Point's market-leading technology on high performance hardware platforms.

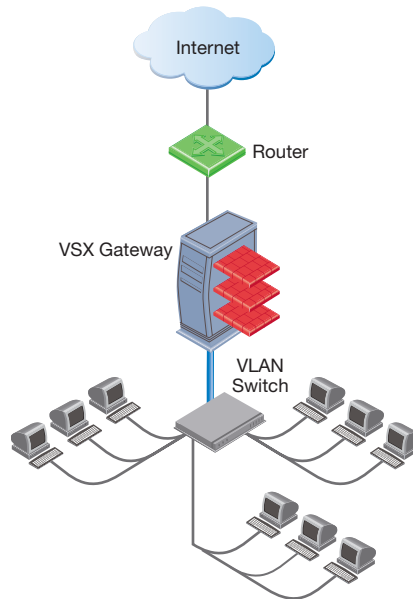


Figure 1: VPN-1 VSX protects up to 250 data center security domains with a single hardware platform.

By using a single platform, customers eliminate the need to invest in and deploy multiple solutions to achieve end-to-end security. In addition, SmartCenter and Provider-1[®], which are based on Check Point's state-of-the-art SMART architecture, provide customers with a centralized console to manage VPN-1 VSX as well as other Check Point gateways maximizing management efficiency.

The SMART architecture enables a rich set of sophisticated management capabilities in Check Point solutions. Starting with core components such as an Integrated Digital Certificate Authority and advanced state table synchronization capabilities, SMART technologies allows Check Point to offer management tools to meet the needs of all organizations, from small businesses to larger distributed enterprises to global service providers.

The Check Point approach offers service providers and enterprises:

- **Scalable Virtualized Architecture**

Comprised of multiple virtualized security domains or Virtual Systems (VS), VPN-1 VSX enables customers to protect hundreds of networks using a single platform. Multiple VSs may be associated with a single physical interface on the gateway using VLAN technology. VPN-1 VSX also provides SmartDefense attack protection capabilities and delivers the highest level of security.



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

■ Wire-Speed Security

In high-bandwidth environments associated with data centers and POPs, where hundreds of applications and users are supported, high performance is of critical importance. This solution delivers secure multi-gigabit throughput because it can be deployed on multiple carrier-class platforms that use Check Point's SecureXL™. SecureXL is an open interface for offloading intensive security operations to third-party hardware or optimized software that meets customer needs by delivering multi-gigabit performance levels and multiple form factors.

■ Non-Stop Security

VPN-1 VSX can deliver non-stop security in data center and POP environments because it can be deployed in a cluster using Check Point's ClusterXL™ technology. ClusterXL ensures that changes made to a policy on the primary gateway are immediately reflected on the secondary gateway. At any given moment, if the primary gateway fails, a standby gateway will take over without interrupting any connections.

■ Unparalleled Protection

Incorporating the same market-leading Stateful Inspection, FireWall-1, VPN-1 VSX supports more than 150 pre-defined applications and protocols out-of-the-box. This includes Microsoft CIFS, SMTP, FTP, HTTP, DNS, telnet traffic, SOAP/XML, instant messaging, peer-to-peer applications, Windows Media, RealVideo, Session Initiation Protocol (SIP), H.323-based services (Voice over IP (VoIP) and NetMeeting), Oracle SQL and ERP.

■ Integrated Protection Against Network and Application Threats

In addition to access control, VPN-1 VSX also delivers protection against known and new network and application level threats using SmartDefense. It provides application-level inspection to protect data and application servers from malicious activity by employing a set of advanced Application Intelligence capabilities that detect and prevent application-level attacks. For example, VPN-1 VSX defends against well-known attacks such as Nimda, Code Red and Cross Site Scripting. Enterprises and service providers can add anti-virus screening, URL filtering and Java security from a broad selection of OPSEC™ (Open Platform for Security) certified products that provide the industry's most proven and comprehensive answer to the increasing number of attacks directed at critical applications.

■ Support for Secure Remote Access Technologies

VPN-1 SecuRemote™ encrypts and authenticates data to protect against eavesdropping and data tampering. VPN-1 SecureClient extends VPN-1 SecuRemote features with a Stateful Inspection firewall for desktop security. Both clients work seamlessly with VPN-1 VSX. This extends the use of the solution as a VPN gateway and makes secure remote access an integrated part of the overall security policy in VLAN environments. All elements of the security policy — including access control, attack protection and user authentication — are strictly enforced, ensuring the highest levels of security down to the remote user.

■ Efficient Enterprise Management with SmartCenter

VPN-1 VSX management is completely integrated into Check Point's security management solutions SmartCenter™ and Provider-1. Administrators can use the Virtual System Creation Wizard to provision a security and SmartDefense policy for a new virtual system in seconds. One-Click technology enables a virtual system to be added seamlessly to a VPN community. The virtual system automatically inherits the appropriate properties and can immediately establish secure IPSec sessions with all other VPN community members.



Intelligent Security



Scenarios

VPN-1 VSX for Data Centers

Until recently, it made perfect sense to deploy an individual firewall in front of each network. This was essential in order to provide a high level of security, however, it was very expensive to deploy and maintain all of the necessary hardware. With VPN-1 VSX, data centers can reduce the number of physically managed devices and still provide the same level of security. By assigning the same Layer-2 connection to virtual firewalls, the design of the network is virtually the same with lower administration overhead. As a result, service providers can downsize the number of physical devices they use while actually hosting more customers.

As the data center market evolves, customers can expect more value-added security services, increasingly efficient and cost-effective infrastructures and new processes that enable data centers to provide services faster and at more competitive costs. In fact, the ability to provide space, power and environmental controls in a data center has already developed into a commodity. As a result, many service providers operating data centers have launched ongoing efforts to attract new customers and differentiate themselves from the competition by providing VPN and firewall services. For instance, a service provider may offer to securely manage their customers' subnets. By installing a VSX Gateway/Cluster between a VLAN switch aggregating traffic to/from customer servers and the service provider Internet link, a Virtual System that provides access control, NAT, VPN, logging, and SmartDefense services can protect each customer subnet.

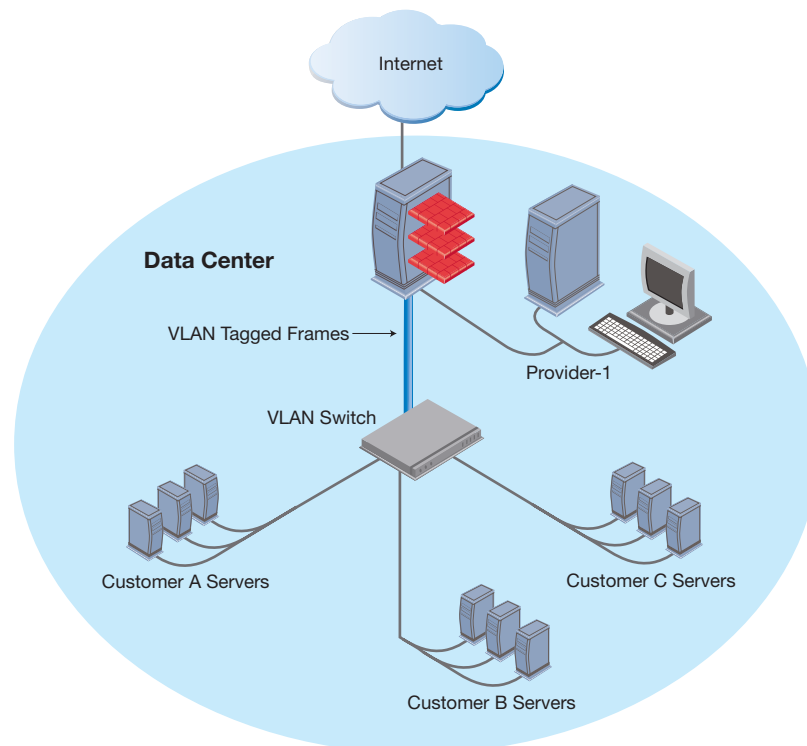
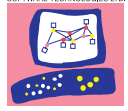


Figure 2: VPN-1 VSX deployed in a Data Center environment.

VPN-1 VSX for Network-Based Security and VPN Services

One of the advantages of a Network-based VPN is that it enables the provisioning of security to a large number of customers in a POP environment and delivers centralized management. Since configuration changes and maintenance are executed by the carrier and not on the customer premises, the service provider is able to increase efficiency and reduce operating costs.

Check Point



We Secure the Internet.

In a network-based security deployment, a VSX Gateway/Cluster can be installed between the service provider Internet link and Edge Router on the boundaries of the service provider Frame Relay/Leased Line/MPLS network. Customer access is controlled using separate Virtual Systems that provides NAT, VPN, logging, SmartDefense and other valued-added services. VPN-1 VSX also enables secure connectivity between customer networks.

VPN-1 VSX also offers secure remote access support by employing VPN-1 SecuRemote, which encrypts and authenticates data to protect against eavesdropping and data tampering. Also, VPN-1 SecureClient extends VPN-1 SecuRemote features with a Stateful Inspection firewall for desktop security. Both clients work seamlessly with Check Point's Application Intelligence. This extends the use of the solution as a VPN gateway and makes secure remote access an integrated part of the overall security policy in a VLAN environment. All elements of the security policy, including access control, attack protection and user authentication, are strictly enforced, ensuring the highest levels of security down to the desktop of a remote user. In addition, overlapping IP domain spaces simplify network provisioning.

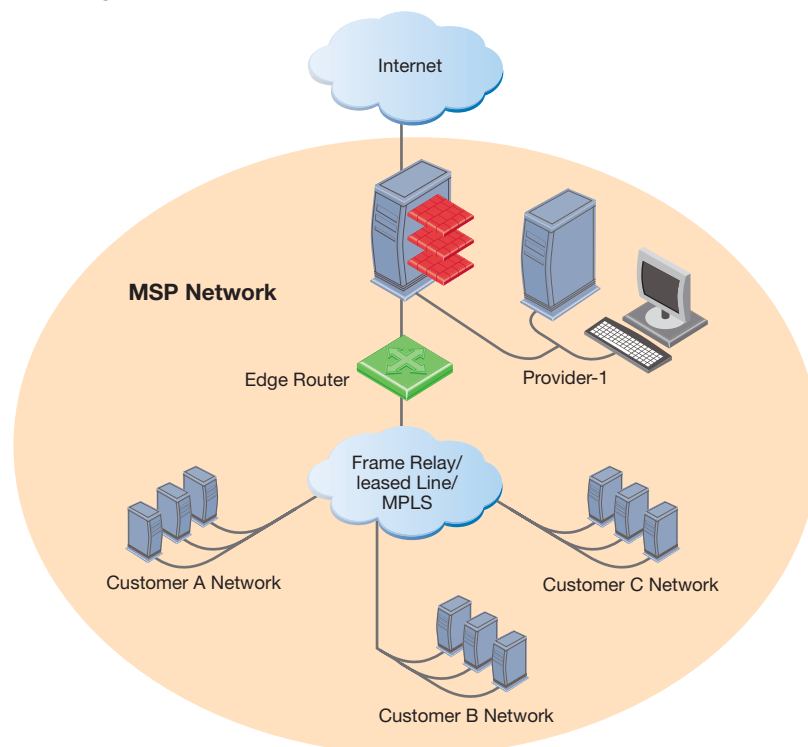


Figure 3: VPN-1 VSX deployed for network-based security and VPN services.

VPN-1 VSX for Enterprise or Campus Networks

Over the years, many organizations have used a demilitarized zone (DMZ) configuration, whereby the VPN gateway is connected via a dedicated interface on the firewall. In this way, VPN traffic can be forwarded after decryption so that access control determinations can be made. The merits of this configuration are that it provides access control of VPN traffic while protecting the VPN gateway from Internet threats, however, these benefits are quickly diminished by network complexity.

As with any non-integrated solution, this architecture requires separate VPN and firewall administration. Deploying two distinct management architectures poses many administrative challenges that affect scalability and network auditing. In fact, the burden of maintaining and upgrading discrete VPN and firewall devices doubles once high availability is deployed. Potentially four or more devices





will require multiple interconnections to ensure that VPN traffic is always properly forwarded to the firewall. Since the firewall and VPN logs are not consolidated, administration can not track network access by user without manually merging and parsing copious data.

With VPN-1 VSX, an enterprise is able to use Virtual Systems to reduce the number of physical devices required. As a result, an enterprise can achieve the highest level of protection from security threats, gain access control over VPN traffic, realize centralized management, simplify routing, consolidate logging, and integrate user authentication within an architecture that is easily scalable.

In addition, an enterprise can use Virtual Systems to segment different business groups, allow the separation of administrative rights across CMAs and their associated Virtual Systems and leverage the ability of the Virtual Systems with VSX to classify the network either by service/function or by network segment.

When an enterprise needs to securely segment a complex LAN (campus network), they must make sure that they can secure communications among the various segments, enforce and maintain a consistent security policy across the entire campus network and monitor for network and application attacks.

Using proven security technology, VPN-1 VSX delivers access control, remote access and attack protection via a single solution that reduces capital investment, reduces administrative overhead, simplifies security policy provisioning and integrates with the existing security infrastructure.

In an Enterprise or Campus deployment, a VSX Gateway/Cluster can be installed between a VLAN switch aggregating traffic to/from multiple subnets and the Enterprise/Campus main Internet link. A separate Virtual System — providing access control, NAT, VPN, logging, and SmartDefense services — protects each subnet. VPN-1 VSX also enables secure connectivity between subnets.

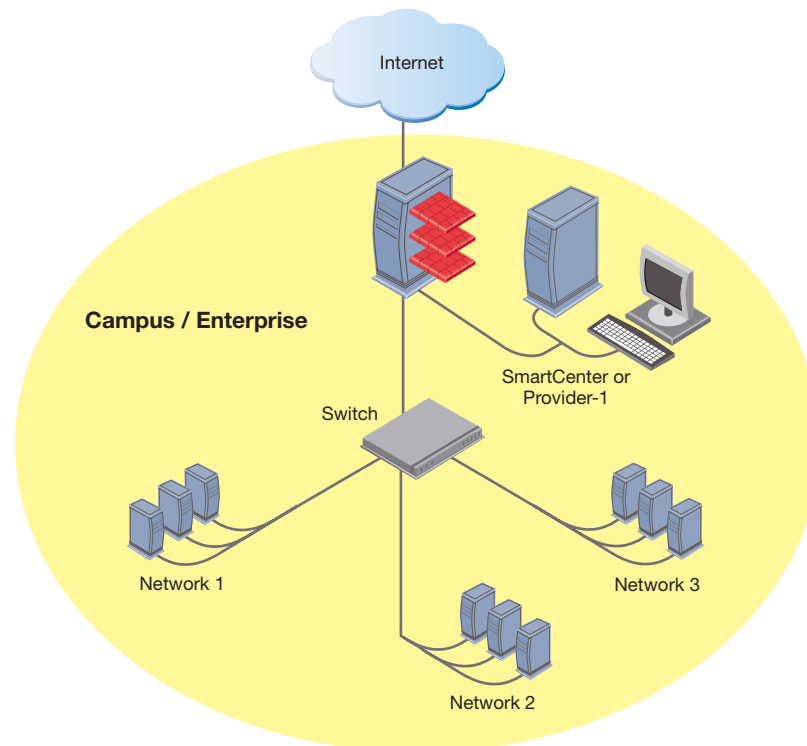


Figure 4: VPN-1 VSX deployed for enterprise or campus networks.



VPN-1 VSX centralizes deployment, SmartCenter centralizes management and Provider-1 can be used for management if each LAN segment requires its own security policy. Also, each segment can have its own security administrators using Provider-1.

For all three scenarios, VPN-1 VSX protects and provides secure access to the hosted applications while SmartCenter or Provider-1 delivers centralized management capabilities, depending on the customer scenario. In addition, VPN-1 VSX offers secure remote access support by employing SecuRemote, which encrypts and authenticates data to protect against eavesdropping and data tampering. Also, VPN-1 SecureClient uses a centralized Policy Server to protect network clients. The Policy Servers may be set up in a distributed configuration for increased availability.

Delivering Network and Application-Level Protection with SmartDefense

Organizations of all sizes, across all industries, face a serious threat of attacks against both networks and critical applications. Network-level attacks attempt to target network components or the firewall directly, while application-level attacks attempt to exploit vulnerabilities in applications running on the network. The increasing sophistication of these threats requires a renewed vigilance on the part of the security manager to actively and intelligently block Internet attacks. A robust and reliable security solution must have the intelligence not only to block all attacks at both the network and application level, but also to provide the security manager with a detailed understanding of the attacks. Useful forensic information combined with real-time security updates delivers better perimeter, internal and Web security and protects the organization from emerging Internet threats.

SmartDefense is a product

Centralized control for network defense

Centralized control for application-level defenses

Response, alerting and tracking configuration

The screenshot shows the SmartDefense configuration interface. On the left is a tree view of configuration objects. The main area is divided into several panels: 'General' (with sub-sections like Denial of Service, IP and ICMP, etc.), 'File and Print Sharing' (with a table of worm patterns), and 'Attack Description' (providing details for a detected CIFS worm). At the bottom, a table displays the attack log.

No.	Date	Time	Product	Attack Name	Interface	Origin	Type	Action	Service	Source
7	1Mar2003	1:11:5	SmartDefense	Larg ping	E90x1	Alaska_member2	Log	Drop	bad.ICMPS	
8	1Mar2003	1:12:13	SmartDefense	Bad TCP sequence	E90x1	California_GW	Log	Drop	snmp	192.168.1
9	1Mar2003	3:11:17	SmartDefense	URL worm	E90x1	Florida_GW	Log	Reject	http	badworm2

Real-time attack information

Forensics and active response

Figure 5: SmartDefense actively protects organizations from all known network and application attacks using Application Intelligence and Stateful Inspection technology.



Check Point

SOFTWARE TECHNOLOGIES LTD.



We Secure the Internet.

offering that enables customers to configure, enforce and update network and application attack defenses. Included with FireWall-1, SmartDefense actively protects organizations from both network and application attacks using Check Point's patented Stateful Inspection and innovative Application Intelligence, both based on INSPECT, the industry's most adaptive and intelligent inspection technology.

SmartDefense not only protects against a range of known attacks, varying from different types of HTTP and Microsoft Networking worms to Distributed Denial-of-Service attacks, but it also incorporates intelligent security technologies that protect against entire categories of emerging or unknown attacks. In addition, SmartDefense integrates with the Check Point SMART Management and reporting infrastructure to provide a single, centralized console for real-time information on attacks as well as attack detection, blocking, logging, auditing and alerting.

SmartDefense provides security managers with a single, centralized point of control against attacks. Attack types include mass-distributed and emerging attacks, like Code Red or Nimda, as well as Denial of Service (DoS), Internet worms, illegal and malformed Internet traffic, and fragmentation attacks. Alerting, tracking and auditing are all configured centrally, providing a complete solution for responding to attacks.

Since keeping security current is a key element of remaining secure, SmartDefense works in conjunction with an ongoing subscription service delivered by Check Point to ensure that the latest information on new and emerging attacks is available to SmartDefense users. These online updates expand the capabilities of SmartDefense, delivering a level of response and flexibility that ASIC-based firewalls are not designed to provide. Subscribing customers get one-click, automatic SmartDefense updates from within SmartDashboard®. When Check Point publishes updates, the SmartCenter management server retrieves new signature patterns, protocol definitions, and attack mitigation solutions from Check Point and distributes them to enforcement modules.

VPN-1 VSX blocks many attacks and provides numerous attack prevention safeguards using SmartDefense. To review detailed documents that demonstrate how Check Point technology successfully prevents attacks at a network's perimeter, internally and at the web, contact your nearest sales representative or visit our website at http://www.checkpoint.com/appint/appint_application_layer.html.

To learn more about Check Point's using SmartDefense technology contact your nearest sales representative or visit our website at: http://www.checkpoint.com/products/downloads/smartdefense_datasheet.pdf

Achieving Centralized Management with SmartCenter and Provider-1

SmartCenter

SmartCenter is Check Point's enterprise management solution for centrally configuring, managing and monitoring multiple VPN-1 enforcement points as well as certified best-of-breed security solutions. SmartCenter leverages Check Point's revolutionary SMART to enable all elements of a security policy to be defined and managed from a single console. This comprehensive approach delivers the industry's lowest total cost of ownership for network security deployments.

SmartCenter is Check Point's flagship management solution and is comprised of an intuitive "dashboard" that enables administrators to centrally define the VPN, firewall and QoS policies. It's also a management server that stores and distributes these different elements of the security policy, providing administrators with enhanced understanding of distributed security deployments. This is combined with automatic policy distribution to deliver greater control, improved security, and enhanced ease of use.





We Secure the Internet.

SmartCenter enables visual management of network security, centralized distribution and inventory of software, real-time security and VPN performance monitoring, powerful integration with LDAP-based directories, and fault tolerance of all management operations. It also enables support for multiple policies, a single database shared among all Virtual Systems, full read/write access for an administrator, logging and reporting for each individual Virtual System and One-Click technology to easily add a Virtual System to the VPN community.

To learn more about Check Point's SmartCenter technology contact your nearest sales representative or visit our website at: http://www.checkpoint.com/products/downloads/smartcenter_datasheet.pdf

Provider-1

Provider-1 is a security management solution designed to meet the unique challenges of service providers and large enterprises. For service providers, it consolidates customer security policies into a centralized policy management architecture that scales to support thousands of customers while minimizing investment in hardware and labor. For a large enterprise, Provider-1 simplifies a complex security policy by segmenting it into more manageable sub-policies to match geographic, functional, or other logical groupings.

With a three-tier, multi-policy security architecture, Provider-1 consists of enforcement points, a management console, and a GUI that delivers a robust mechanism for creating a single security policy and automatically distributing it to multiple enforcement points. However, service providers and large enterprises require an infrastructure for managing more than just a single policy. They need to centrally manage multiple distinct policies simultaneously.

Global policies are security templates that can be applied to multiple security policies. Global policies eliminate the need to create identical policies for each customer individually. Network objects that get defined in global policies are known as "global objects" and may be granularly assigned to CMAs enabling administrators to formulate granular security policies for multiple customers in a single operation. This feature greatly improves management efficiency.

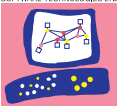
The Administrator Manager provides a flexible way to distribute management responsibility among a group of security administrators. Responsibility may be divided according to CMAs, or even according to specific functional tasks within CMAs such as VPN/security, log monitoring, QoS, etc. Customers may also be granted access to certain tasks that are managed using the Administrator Manager. One of these tasks include read and write access to their user database.

Check Point's Total Availability Management system delivers a fully redundant management infrastructure ensuring that connectivity to customers is never lost. Numerous Multi Domain Servers (MDSs) can be deployed in a single NOC, or in various NOCs around the world. Each MDS is connected to others by a "nervous system" that automatically synchronizes customer and administrator data so that each MDS acts as a backup server to others. These interconnected, mutually redundant MDSs form a robust management system providing non-stop access without the need to deploy dedicated redundant hardware and software.

To learn more about Check Point's Provider-1 technology contact your nearest sales representative or visit our website at: http://www.checkpoint.com/products/downloads/Provider1_DataSheet.pdf



Intelligent Security

Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.

Conclusion

With an increasingly decentralized workforce and the rising need to elevate the level of information security, enterprises and service providers have been prompted to deploy sophisticated security infrastructures that are becoming more and more complex. If even one small part of the infrastructure isn't completely secure, then the entire organization is at risk. As a result, enterprises and service providers are taking an integrated network and application approach providing protection that addresses perimeter, internal and Web security. Since a piecemeal approach leads to a high level of frustration and difficulty when managing and maintaining disparate product vendors, specialized security experts, access providers, and systems integrators, enterprises and service providers are seeking an integrated solution that delivers access control, remote access and attack protection from a single solution.

Network-based solutions meet these basic requirements and enable service providers and enterprises to leverage their existing security infrastructure, reduce capital investments, cut administrative overhead costs, and simplify policy provisioning.

Demonstrating its leadership in information security, Check Point offers the industry's only solution to deliver integrated access control, network and application-level attack protection, and client security in a virtual environment — with up to 250 virtual systems running on a single platform. Enhanced to include Check Point's best-in-class Application Intelligence technology, SmartDefense attack protection and VPN-1 SecureClient remote access as well as desktop security, VPN-1 VSX equips service providers and enterprises with integrated end-to-end protection against dynamic Internet threats that is supported on a wide range of platforms, including Check Point SecurePlatform, Crossbeam X40, Nortel ASF 5114 and Nortel ASF 5124. As a result, enterprises and service providers will be able to strengthen their security while taking advantage of the cost efficiencies of virtualization, which eliminates the need to invest in additional infrastructure.

About Check Point Software Technologies

Check Point Software Technologies is the worldwide leader in securing the Internet. It is the confirmed market leader of both the worldwide VPN and firewall markets. Check Point provides Intelligent Security Solutions for Perimeter, Internal and Web Security. Based on INSPECT, the most adaptive and intelligent inspection technology and, SMART Management, which provides the lowest TCO for managing a security infrastructure, Check Point's solutions are the most reliable and widely deployed worldwide. Check Point solutions are sold, integrated and serviced by a network of 1,900 certified partners in 86 countries. For more information, please call us at (800) 429-4391 or (650) 628-2000 or visit us on the Web at <http://www.checkpoint.com> or at <http://www.opsec.com>.

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:
800 Bridge Parkway
Redwood City, CA 94065
Tel: 800-429-4391; 650-628-2000
Fax: 650-654-4233
URL: <http://www.checkpoint.com>

© 2004 Check Point Software Technologies Ltd. All rights reserved. Check Point, Application Intelligence, Check Point Express, the Check Point logo, ClusterXL, ConnectControl, FireWall-1, FireWall-1 GX, FireWall-1 SecureServer, FireWall-1 XL, FloodGate-1, INSPECT, INSPECT XL, InterSpect, IQ Engine, Open Security Extension, OPSEC, Provider-1, Safe@Office, SecureKnowledge, SecurePlatform, SecureXL, SiteManager-1, SmartCenter, SmartCenter Pro, SmartDashboard, SmartDefense, SmartLSM, SmartMap, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, UAM, User-to-Address Mapping, UserAuthority, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, and VPN-1 VSX are trademarks 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.

P/N 501307

