



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.



White Paper

Virtualized Network Security with VPN-1 Power VSX



Intelligent Security

Check Point protects every part of your network—perimeter, internal, Web—to keep your information resources safe, accessible, and easy to manage.

Contents

Executive summary	3
Introduction to virtualization	4
Check Point VPN-1 Power VSX	4
Components virtualized by VPN-1 Power VSX code	5
Layer-2 security	5
ARP poisoning	6
VLAN hopping	6
Platforms	6
Crossbeam Systems	7
Check Point SecurePlatform	7
Virtual network environment	7
Application layer protection	8
Availability, reliability, and scalability	8
Quality of Service	10
Secure provisioning	10
Secure Management Architecture	11
Management challenges	11
Security classes	13
Permission enforcement	14
Conclusion	15

Executive summary

Network complexity is growing rapidly. Dynamic business requirements, mergers, spinoffs, new services, new business units, new threats, and compliance considerations are driving an ever-increasing investment in network resources, equipment, and invasive infrastructure changes. The result is often a higher cost structure combined with lower network and service availability.

Companies are realizing the advantages of information technology virtualization with the adoption of MPLS VPNs, VLANs, blade architectures, and virtualized servers. More recently, virtualization has been applied to network security in order to improve security services and manageability while reducing capital costs.

Virtualized network security can help enterprises and service providers cope with the dynamic nature of business by providing a very flexible infrastructure. Organizations can achieve an overall reduction in costs by reducing the hardware investment and administrative complexity of securing data centers, points of presence, core networks, and large segmented networks.

Check Point's virtualized network security solution, VPN-1® Power VSX™, is engineered from its VPN-1 Power physical gateway technology to add the benefits of virtualization to the industry's most intelligent and manageable firewall, secure remote access, and intrusion prevention solution. By eliminating the need for a physical device for each security gateway in a virtualized network environment, VPN-1 Power VSX reduces hardware acquisition and maintenance costs, rack-space requirements, security provisioning labor and policy administration, and human error.

Introduction to virtualization

Virtualization is the separation of functionality from the physical implementation of hardware technology. It makes a centrally managed physical environment appear to be many autonomous logical environments or systems. Each autonomous system provides the same services and operates as if it were a completely isolated physical entity. Each logical entity within a system is called a virtual device. Virtual devices are fully functional and completely segregated environments, which have the ability to operate and appear as physical devices. Their autonomy is complete at any level of the solution—connectivity, software, or management.

Privacy is one of the primary success factors for secure virtual environments. Individual physical network devices, such as routers, switches, monitoring systems, and various security solutions, each manage a private set of service tables, routing information corresponding to different network interfaces, Layer-2 forwarding, translation tables, and many other application-dependent data structures. It is imperative that a virtual network device ensure compliance with this degree of separation.

Virtualization addresses multiple areas: infrastructure (including interfaces, networking, and configuration), security (firewall, VPN, intrusion prevention), and management. A basic requirement for a virtualized security solution is its adaptability. Security is required at different parts of the infrastructure—at the perimeter, at the core, as a service, or at any other region of the network. Each region has different needs, with different pain points. A virtualized security solution must be able to integrate with various areas of the network without imposing connectivity restrictions or painful changes.

Check Point VPN-1 Power VSX

Check Point designed the VPN-1® Power VSX™ virtualized security gateway to add the benefits of virtualization to the advantages of its award-winning VPN-1 Power network security gateways. The solution was architected to meet several key objectives:

- **Security**—each virtual device must provide the highest quality network security that enterprises expect from Check Point's physical security solutions
- **Segregation**—each virtual device must be a private domain, based on complete logical separation between devices
- **Scalability and flexibility**—a VPN-1 Power VSX deployment must be agnostic to the network infrastructure and provide a scalable virtual environment that can adapt to any network design
- **Resiliency**—the solution must maintain business continuity, service integrity, and network predictability
- **Manageability**—the solution must be simple and intuitive to administer

VPN-1 Power VSX provides a completely virtualized model of a secure infrastructure, with high scalability and availability, environmental integration, quality of service (QoS) support, and permission management. To ensure privacy between domains, the solution utilizes the “bad neighbor” concept, providing complete separation with no exceptions. As a result, VPN-1 Power VSX is not susceptible to threats such as ARP poisoning and VLAN hopping. Private kernel tables and network components, such as routing tables, are maintained for each virtual device.

Components virtualized by VPN-1 Power VSX code

State table—state tables store configuration and runtime information, such as network address translation (NAT) rules, active connections, and active IPsec tunnels

Security and VPN policies—each virtual entity enforces its own security and VPN policies (including INSPECT™ code), which are individually downloaded from the management server and kept separately on disk and in the kernel

Configuration data—each virtual entity is configured separately and maintains its own configuration tables, such as SmartDefense™ settings and TCP/UDP timeouts

Routing tables—each virtual entity maintains a completely private virtual routing and forwarding (VRF) table. A VRF is created automatically for each component and operates independently, as if it were a physical device. However, unlike MPLS, VRFs cannot be shared among multiple entities

ARP tables—VPN-1 Power VSX manages address resolution information, based on the interfaces on which the information was learned. The ARP interface context allows the solution to associate ARP information with specific virtual systems (VSs)

Logging information—a virtual entity can be configured to log its operations. Each VS, depending on the management model, can have its own separate administrators. Alternately, a single administrator can be defined for groups of virtual systems, according to requirements

This type of model is consistent across the different virtual devices: router, switch, system, and firewall.

By enabling a complete virtual network environment, VPN-1 Power VSX simplifies the network and enhances the security zone with a more coherent structure. Layer-2 services, such as VLANs and VLAN trunks, are widely accepted and deployed across all types of networks. As part of the end-to-end security approach taken by VPN-1 Power VSX, Layer-2 threats are also being dealt with.

Layer-2 security

Layer-2 networks are susceptible to denial of service and privacy threats, which can be dealt with by means of proper device configuration. The Layer-2 security threats that potentially undermine virtual solutions are ARP poisoning and VLAN hopping attacks.

ARP poisoning

ARP poisoning is a method by which attackers transmit fake ARP packets in the broadcast domain. Such packets may potentially modify the operating system ARP cache, redirecting traffic to an unauthorized destination. Only attackers residing in the same broadcast domain can launch such attacks. VPN-1 Power VSX mitigates this general problem by isolating ARP information and classifying it based on the interface—physical or logical—by which the ARP packets were received. By creating interface-savvy ARP entries, the solution enforces VS-specific Layer-2 security.

VLAN hopping

VLAN hopping is a method for forwarding frames from one VLAN to another. Double 802.1q encapsulation is an attack used to force the VLAN driver to deencapsulate the 802.1q information a second time and reassign the frame to another VLAN.

VPN-1 Power VSX is not susceptible to such threats because it validates the source of the 802.1q frame. When the driver of the VPN-1 Power VSX platform receives the 802.1q frame, it identifies two items—the 802.1 tags and the interface they came through. While deencapsulating the 802.1q tags, the driver attaches the VLAN ID to the interface name. For example, ETH0 becomes ETH0.100. In a scenario in which the driver receives a double encapsulated frame, the result may be ETH0.100.101, an interface that is not assigned to any virtual device.

By default, Layer-2 security verification is enforced across all virtual devices. VPN-1 Power VSX creates each device with security as the priority, resulting in a fully functional and secured network environment. The different components allow security and network engineers to design a secured infrastructure. VPN-1 Power VSX also deals with the many security tasks, such as hardening, provisioning, and health monitoring, required to completely secure the network environment. However, it greatly reduces the number of trivial issues and frees engineering resources to deal with other security tasks. The different virtual devices provide a secure virtual network environment, complying with both the familiar behavior of switches, routers, and firewalls, and at the same time enforcing strict security standards. Each virtual device is secured via FireWall-1® INSPECT technology. The INSPECT code is used to automatically enforce security per virtual device, protecting and alerting the administrator accordingly.

Platforms

Hardware platform support plays a key role in the design process of virtualized security. VPN-1 Power VSX is supported by multiple hardware platform operating systems, including Crossbeam and Check Point SecurePlatform™. Each platform offers a uniquely tailored solution for virtualization. Platforms vary in performance, load sharing, top-down redundancy, and other characteristics, allowing each organization to customize the solution to its network and/or service needs.

Crossbeam Systems

Crossbeam Systems provides custom hardware, designed for a highly redundant environment. Every part of the solution is redundant—dual power supplies, dual fans, multiple application modules, dual network processors, and dual box configuration. Crossbeam supports SecureXL™ software-based high availability and load sharing as well as transparent load sharing, creating an environment for availability and high performance. (For more details, please refer to Crossbeam's documentation.)

Check Point SecurePlatform

SecurePlatform is an optimized, secure OS running on open systems hardware. It optimizes resource allocation of CPU and memory usage and accelerates VPN performance. (For more details, please refer to the SecurePlatform documentation.)

Virtual network environment

When introducing a new service into the network, the following are generally taken into account:

- Security implications
- Infrastructure requirements (IP scheme, routing design, and physical connectivity)
- Management requirements

VPN-1 Power VSX addresses these requirements by creating a virtual network environment. This environment allows the building of multiple virtual infrastructures comprising virtualized traditional network elements, such as virtual switches, routers, firewalls, firewalls in native Bridge mode, and cables. The different elements are designed to integrate with the infrastructure, in Layer 2, Layer 3, or both.

Virtual systems in Bridge mode are core-side security devices. The ability to deploy virtual systems in Bridge mode allows administrators to introduce security into the network with few or no changes to the existing topology or network settings. Virtual systems in Bridge mode are designed to integrate into heterogeneous environments, which might support nonstandard, but heavily utilized protocols. Support for all spanning tree protocols and the VLAN management protocol are recognized by the Layer-2 virtual device and VLAN IDs are kept intact. In addition, IT integration is transparent and the flow of traffic is controlled by the network, while virtual systems secure the assets, establish structure, and manage the security information of the network.

VPN-1 Power VSX supports two types of Layer-3 virtual devices: virtual systems and virtual routers. To accommodate the organic nature of the network and access paths, each Layer-3 device fully supports both unicast and multicast routing protocols (BGP-4, OSPF, PIM-DM, PIM-SM, and RIP). Each virtual device is full featured and acts as a physical routing device, with complete support for advertisement methods, attributes, boundaries, limits, and routing filters. Relationships can be established among all types of virtual devices, extending service resilience and the level of network integration.

Security should not impinge on network performance: it should allow information packets to flow with as little interruption as possible. VPN-1 Power VSX provides an enriched network environment, ensuring secure connectivity.

Application layer protection

Today, most attacks take advantage of open and legitimate ports. For example, CIFS, HTTP, VoIP, and other protocols are susceptible to manipulation as well as denial of service (DoS), virus, and worm attacks.

Unlike reactive, signature-based deep-inspection technology, Check Point's SmartDefense proactive security technology defends against new attacks and variations as they appear. For example, this means that worms are stopped before they can affect networks. SmartDefense is continuously being updated with new security protections against potential and existing threats.

Besides mitigating worm threats, SmartDefense is beneficial to the integrity of the network on several other levels. For instance, because it is a network-aware solution, it can secure complex environments such as those using VoIP applications. The complicated nature of voice protocols makes them extremely difficult to secure. However, unlike other intrusion prevention approaches, SmartDefense not only inspects basic VoIP traffic but also considers the voice network design, offering a solution that can deliver fraud detection and security inspection of voice protocols. It also provides detailed forensics information.

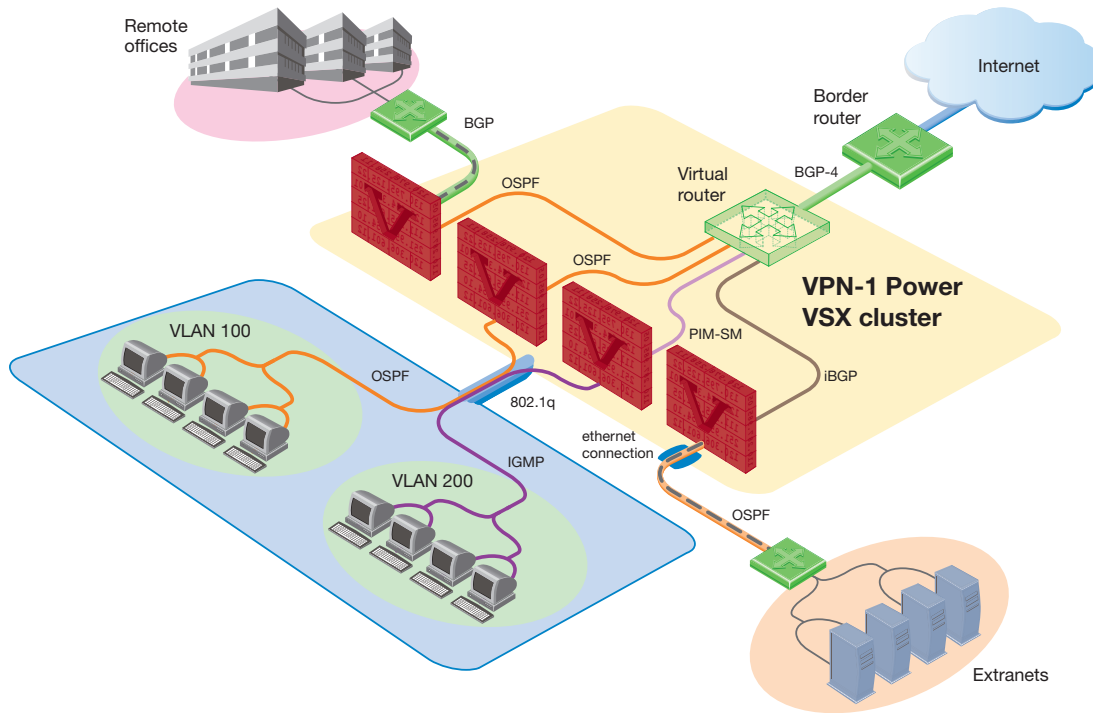
Virtualization of SmartDefense ensures that enterprises do not give up the security benefits of Check Point's advanced intrusion prevention capabilities when they adopt VPN-1 Power VSX.

Availability, reliability, and scalability

Service availability and infrastructure reliability are critical factors in the overall strength of the network. Virtualized security gateways based on a flat design would limit scalability. An example would be a product in which the daemons are duplicated and where all configuration data and information is stored in a single structure. In contrast, VPN-1 Power VSX clustering solutions create a highly scalable and available security platform with in-depth analysis of system status and health.

Linear growth clustering in VPN-1 Power VSX provides highly efficient distribution of virtual systems on different members of a physical gateway cluster. Capacity increases are proportional to increases in the number of members in a cluster. The result is the greatest effective capacity for a given hardware investment, combining cost efficiency and network security scalability.

VPN-1 Power VSX clustering is based on Check Point's patented ClusterXL[®] load sharing technology, which supports very efficient automatic or configurable distribution of traffic among cluster members and substantially reduces synchronization traffic. In addition to hardware efficiency, this clustering technology also provides real-time monitoring of traffic load distribution. Scalability is further enhanced by configurable resource controls that ensure that the consumption of CPU resources by each virtual system is optimal for overall network security. Resource controls can limit the CPU time available to a lower priority virtual system, assign more capacity to mission-critical virtual systems, and mitigate the impact that a DoS attack on one virtual system has on the other virtual systems.



A highly available, virtualized solution faces a number of challenges. Issues such as convergence times, failover times, ripple effects, and route availability are some of the considerations that must be taken into account.

Unicast routing protocols, like BGP, OSPF, and RIP, increase availability by enhancing the flexibility and the number of available paths. The ability to participate in the routing domain is not sufficient. Virtual routing environment failure and its consequences must be considered as a major threat. VPN-1 Power VSX poses no restrictions on either design or protocol operations—the base point is one cluster, one visible network device. When it comes to routing protocols, several issues can affect the network. They include adjacencies/peering status, dynamic route changes, and link states.

Each protocol state is associated with an expected response, which affects the network in numerous ways. Effects include topology changes, route withdrawal, unnecessary resource allocation, and failover time. VPN-1 Power VSX is designed to integrate into an existing network infrastructure. The integrity of the network environment and the ties it maintains with the cluster, such as routing information and protocol relationships, are an important part of the VPN-1 Power VSX cluster solution.

Convergence time is problematic when dealing with resiliency. Considerations such as the number of routers in a BGP peering design, number of advertised routes, OSPF area, and route advertisement patterns are just some of the issues that must be accounted for to maintain a reliable, available network.

Virtual system clusters appear to the network infrastructure as a single logical device. Such an approach dramatically reduces both the impact of a failure and the required maintenance on the network. The ability to appear as a single entity allows VPN-1 Power VSX to be both nondisruptive and nonintrusive.

VPN-1 Power VSX addresses connection state and convergence issues through the following mechanisms:

- **Cluster and protocol integration**—routing protocols recognize the virtual IPs as the primary interface addresses and all protocol-related messages are issued accordingly
- **Continuous routing table synchronization**
- **Recreation of protocol-established relationships**—hitless restart protocol extensions have been integrated with the cluster mechanism to avoid unnecessary ripple effects

Quality of Service

Quality of Service (QoS) enforcement with VPN-1 Power VSX supports the Differentiated Services architecture and allows assigning different transmission characteristics to different classes of service. The major characteristics that are controllable are latency and bandwidth allocation. Without QoS enforcement, different traffic types are given equal priority and handled in a simple FIFO (first in, first out) manner. When the network or gateway is congested, all traffic types suffer the same degree of latency and dropped packets. Also, high-volume traffic may starve low-volume traffic of bandwidth.

With the QoS for VPN-1 Power VSX, the special requirements of different traffic types can be met. For example, latency-sensitive traffic can be given preference over other types of traffic; traffic insensitive to dropped packets will suffer fewer drops than other types of traffic; and high-volume traffic that consumes bandwidth will be limited during times of congestion.

Secure provisioning

VPN-1 Power VSX modules are provisioned by Check Point's traditional central management platforms, such as Provider-1® and SmartCenter™. The management tools perform some of the initial configuration tasks locally on the enforcement module, which requires either direct access to the machine or some sort of remote shell access. Services, such as routing protocols and Certificate Authority server management, are examples of two tasks that require access to the module.

Every type of connection directly established with the module is a potential threat. VPN-1 Power VSX mitigates the risk via the internal access structure of the module. Two methods of access are allowed: physical server access or via Secure Shell access. Both methods require the presence of authentication credentials and specific network access. Only the owner of the VPN-1 Power VSX cluster is authorized to access the module. Each machine administrator is issued a private set of such credentials. VPN-1 Power VSX does not allow separate Secure Shell access with individual virtual devices. Moreover, the various virtual devices do not have servers running, which would allow such access. The ability to access the machine is dependent on the virtual management system.

The security for provisioning VPN-1 Power VSX devices is provided by a dedicated virtual system that preserves all the information from its synchronization operations. VPN-1 Power VSX management enforces inspection rules, protecting it from external connections through physical interfaces, or virtual devices, if available. All management operations must be preapproved by VPN-1 Power VSX management, thus no SNMP, SSH, or any other management protocols can communicate with virtual gateways unless they have been authorized to communicate and only if their communications are audited.

The combination of authentication credentials and specific network access establishes an access structure that supports an organization's security policy while providing the flexibility to support the organizational management structure.

Secure Management Architecture

Based on Check Point's Secure Management Architecture (SMART), Provider-1 delivers a management solution for control and security, offering:

- Scalability to accommodate a growing number of devices
- Service and associate information
- A multifaceted view of the network

Extranet services, global VPNs, remote access connections, secure DMZs, VoIP telephony, and Web server farms are just a few of the services that require security management. Each service maintains a separate set of security specifications, comprising application version, device type and grade, IP scheme, management teams, network architecture, policy, and service level agreement (SLA). These attributes must be taken into account, accommodated, and represented. Provider-1 views VPN-1 Power VSX as just another firewall in the Check Point environment, allowing a single solution to manage the entire network, and consequently broadening the security perspective of the organization.

Management challenges

One of the most important aspects of a successful security deployment is its overall manageability. The degree to which an administrator can easily manage a security deployment directly affects the return on investment of the solution and the overall IT costs of the organization. Management can be broken down into several categories:

Device management—a large and growing number of machines require intelligent, efficient management

Security policy management—the continuous growth of an enterprise's security policy, results in various security issues. The overall quality of security of the network diminishes. The size of the policy hampers the ability to detect existing and potential security holes. The introduction of new security rules becomes an extremely difficult task, with a high probability for mistakes and unexpected service outages

Security information management—the amount of security information generated by the firewall infrastructure is extremely large. The inability to manage and utilize the security information affects troubleshooting. Due to the amount of information, troubleshooting time becomes longer and more difficult, resulting in longer service outages

Security trend analysis—security trend analysis also becomes more difficult. Due to the enormous amount and detailed security information generated by the different devices, security engineers cannot successfully analyze the information and take preemptive steps based on the behavior observed

VPN architecture—creating multilayer VPN networks is a common practice in enterprise and service provider networks. Mobile users and remote offices commonly use VPN technology to communicate with the office resources

Permission management—the permission structure reflects the organization's structure. Departments, regions, services, or any other class of the network can be considered separate groups, with different sets of permissions. The inability to match tailored policies to each of these different groups creates security problems

Overall, security management provides the ability to view the network as a multifaceted entity comprising:

- Device management
- Service management
- Information management
- Policy management
- Organizational structure

The association between different management domains and a service, a network area, or any class of the organization exponentially increases the required network control and security. Management-domain classification limits the management scope of each security domain—in terms of security information management, security policy, and management team's responsibility—as follows:

- **Security information management**—each security domain manages a specific portion of the security-generated data. The relevant engineering group receives focused information, while still having the ability to perform cross-domain forensic analysis, by owning the proper credentials. Such an approach increases the security control and at the same time simplifies the troubleshooting process
- **Security policy**—each domain manages only a small number of relevant security policies. Distributing the policy across multiple security domains allows the engineers to better understand and manage the policy. Because they no longer have to deal with hundreds of policy lines, the risk of overlooking security holes is reduced
- **Policy per team**—relating the policies to the organizational structure allows specific teams to get access based on responsibility scope and level of skills, limiting the risk of human errors and focusing the engineering group's tasks

The Provider-1 management model applies to each section of the network. The perimeter and internal networks tend to be the largest and most complex areas of the overall network. Both areas commonly host a number of different services and networks, corresponding to separate security classes.

Security classes

A security class is a subset of a security area and may be as small as a single VLAN, a service, or a number of services. The perimeter consists of a large number of security classes. DMZs, extranets, Internet access, remote access, and remote office connections are examples of the different classes present on the outer security ring—the perimeter. Due to the ever-growing number of services and network access points, the amount of security devices grows accordingly.

The inner security ring is responsible for securing all the internal resources, such as buildings, departments, servers, and VLANs. The internal network design poses many challenges for security policy designers.

The large number of devices, in conjunction with the numerous services and security classes, necessitates an exceedingly complex security design and creates potential security holes.

The use of VPN-1 Power VSX and Provider-1 to address the different security areas allows engineers to reduce the number of machines, while distributing the services across a larger number of firewalls. The realization of class-based security becomes simple when using VPN-1 Power VSX. Even though class-based security involves network and security design, security enforcement, and management, VPN-1 Power VSX and Provider-1 are equipped to migrate a complex design into class-based security domains.

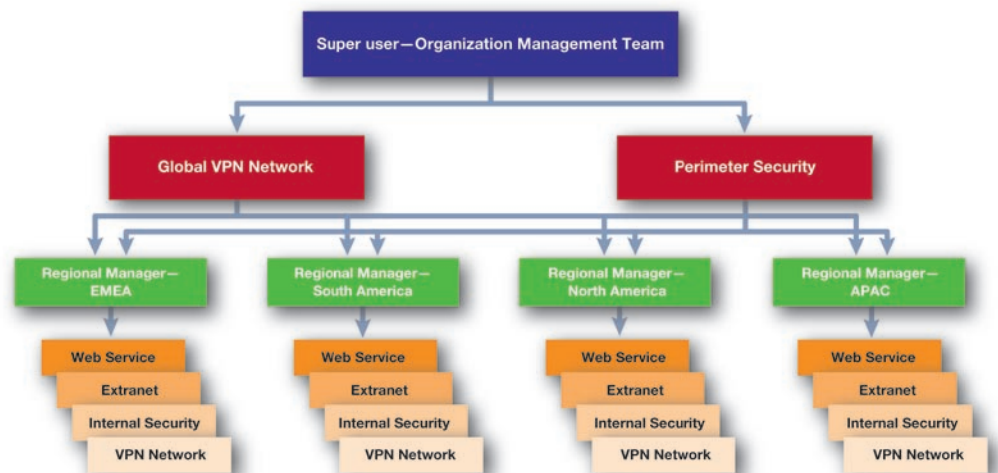
Traditional designs define one or several large firewalls hosting multiple unrelated services and networks that simplify a geographic profile. In general, such profiles are created for practical reasons, such as the number of physical devices required for a class-based security design. Consequently, large and unreadable policies are created and unmanageable volumes of security information are generated. A virtual firewall removes this traditional limitation. It provides the required flexibility and security measures, allowing the enforcement of service-specific security policies, while complying with the specific connectivity requirements of the network class.

In order to conform to such design requirements, Provider-1 accommodates all types of security machines, virtual and physical. Provider-1 interacts with virtual firewalls and allows spanning multiple virtual firewalls across multiple Customer Management Add-ons (CMAs) for complete independent management, based on the specific requirements of the service. End-to-end separation is traditionally part of the Provider-1 architecture. Each CMA is composed of all the components of a management server including a private set of configuration files, a separate user database, and separate security logs.

Permission enforcement

Permission enforcement is a major factor in the overall security of an organization. The ability to comply with the organizational and the permission structure is imperative for the network's integrity. For the most part, permission levels are designed based on hierarchies and group classification. The permission structure must be flexible enough to comply with the different and unique requirements of each organization. VPN-1 Power VSX and Provider-1 create an environment in which private management domains can correspond to any type of classification dictated by the design: service, function, office, region, country, and so forth.

The following schema provides an example for a permission structure:



The idea is to create a structured and self-monitored organization. Each layer is responsible for a specific portion of the network. The model describes the organization's responsibility structure. The example provided describes an organizational permission hierarchy. The structure correlates to services, mandates, and geographical locations. Each level is constructed of either one or more classes:

- The most basic level represents a country or a city
- Second level represents a region
- Third level represents global services
- Fourth level represents a Security Council

The model allows the organization to enforce and monitor security at different levels on the organizational hierarchy. Each level may be responsible for an extranet, function, internal security, Web services, or any other likely service. Each team polices the network, based on organizational security guidelines. In practice, each local management team interprets the guidelines differently and generates a policy based on their security knowledge.

On the second level, regional security managers comprise the permission structure. This team is built of senior security engineers. Regional security managers are responsible for monitoring the security enforced at each of the regional classes and acting as an oversight body. A second objective is to create a base policy, which the class teams will not control. This base policy reflects organization security guidelines, specified by the Security Council (discussed later).

Level three consists of the two major services—VPN and Perimeter Access Security. Although Perimeter Access Security and VPN are handled by the local class teams, each country and each region is considered autonomous. The two teams are global teams, responsible for securely connecting the different autonomous units into a global network and overseeing the regional managers.

At the highest level is the organizational management team that acts as the Security Council, which consists of highly experienced security specialists, who perform trend analysis and security forensics across the entire network. The objective of this team is to lead the organization's security strategy and to set the guidelines and directives for policy, architecture, and overall security. The council is the only level with unrestricted control and view of the network policies and different security data (audit, security logs, etc).

This hierarchical model not only allows for a more efficient operation but also creates a fully monitored structure, in which each level is monitored. This degree of classification allows the different teams to focus their efforts on managing the service for which they are responsible. The combination of Provider-1 permission structure and global policies allows this structure to be enforced, without assigning unnecessary permissions to teams that are not involved with a given topic. VPN-1 Power VSX plays an important role in the enforcement of this model. In general, traditional enforcement assigns dedicated firewall machines, based on network design, rather than on the service or security structure. Such a model concentrates unrelated services within the same management system, causing permission oversubscription. VPN-1 Power VSX allows the permission structure to be maintained, regardless of its physical location, by logically classifying the services into multiple virtual security domains.

Conclusion

Virtualization is an approach that can be found in many areas of information technology. It facilitates scalability and flexibility and removes many of the boundaries imposed by physical implementations.

VPN-1 Power VSX provides a full-featured, virtualized framework for security. It offers highly efficient scalability, transparent failover, fully virtualized availability of security and network devices, complete support for advanced networking protocols, and multitier virtualized management. As an infrastructure solution, VPN-1 Power VSX enforces both network security and privacy to protect neighboring security domains.

With VPN-1 Power VSX, organizations can react more quickly and efficiently to shifts in their businesses. Although this translates into significant cost savings, the greater benefit is helping the organization adapt more quickly and effectively to the ever-changing security threat landscape.

About Check Point Software Technologies Ltd.

Check Point Software Technologies Ltd. (www.checkpoint.com) is a leader in securing the Internet. It is a market leader in the worldwide enterprise firewall, consumer Internet security and VPN markets. Through its NGX platform, the company delivers a unified security architecture for a broad range of perimeter, internal, Web, and endpoint security solutions that protect business communications and resources for corporate networks and applications, remote employees, branch offices and partner extranets. The company's ZoneAlarm Internet Security Suite and additional consumer security solutions are among the highest rated in the industry today, proactively protecting millions of people from hackers, spyware, viruses and identity theft. Extending the power of the Check Point solution is its Open Platform for Security (OPSEC), the industry's framework and alliance for integration and interoperability with "best-of-breed" solutions from hundreds of leading companies. Check Point solutions are sold, integrated and serviced by a network of thousands of Check Point partners around the world and its customers include 100 percent of Fortune 100 companies and tens of thousands of businesses and organizations of all sizes.

CHECK POINT OFFICES

Worldwide Headquarters

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

©2003–2006 Check Point Software Technologies Ltd. All rights reserved. Check Point, AlertAdvisor, Application Intelligence, Check Point Express, Check Point Express CI, the Check Point logo, ClusterXL, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Hacker ID, IMsecure, INSPECT, INSPECT XL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IQ Engine, MailSafe, NG, NGX, Open Security Extension, OPSEC, OSFirewall, Policy Lifecycle Management, Provider-1, Safe@Home, Safe@Office, SecureClient, SecureClient Mobile, SecureKnowledge, SecurePlatform, SecurePlatform Pro, SecuRemote, SecureServer, SecureUpdate, SecureXL, SecureXL Turbocard, SiteManager-1, SmartCenter, SmartCenter Express, SmartCenter Power, SmartCenter Pro, SmartCenter UTM, SmartConsole, SmartDashboard, SmartDefense, SmartDefense Advisor, Smarter Security, SmartLSM, SmartMap, SmartPortal, SmartUpdate, SmartView, SmartView Monitor, SmartView Reporter, SmartView Status, SmartViewTracker, SofaWare, SSL Network Extender, Stateful Clustering, TrueVector, Turbocard, UAM, UserAuthority, User-to-Address Mapping, VPN-1, VPN-1 Accelerator Card, VPN-1 Edge, VPN-1 Express, VPN-1 Express CI, VPN-1 Power, VPN-1 Power VSX, VPN-1 Pro, VPN-1 SecureClient, VPN-1 SecuRemote, VPN-1 SecureServer, VPN-1 UTM, VPN-1 UTM Edge, VPN-1 VSX, Web Intelligence, ZoneAlarm, ZoneAlarm Anti-Spyware, ZoneAlarm Antivirus, ZoneAlarm Internet Security Suite, ZoneAlarm Pro, ZoneAlarm Secure Wireless Router, Zone Labs, and the Zone Labs logo 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, 5,835,726, 6,496,935, 6,873,988, and 6,850,943 and may be protected by other U.S. Patents, foreign patents, or pending applications.

December 6, 2006 P/N 501926



Check Point
SOFTWARE TECHNOLOGIES LTD.

We Secure the Internet.