

VPN-1 VSX

PRODUCT FEATURES:

- Supports 250 comprehensive security policies on a single hardware platform
- Delivers SmartDefense protection against network and application-level threats
- Supports VPN-1 SecureClient and VPN-1 SecuRemote
- Simple, template-based security provisioning process
- Available on carrier-class platforms
- SMART Management for maximum efficiency

PRODUCT BENEFITS:

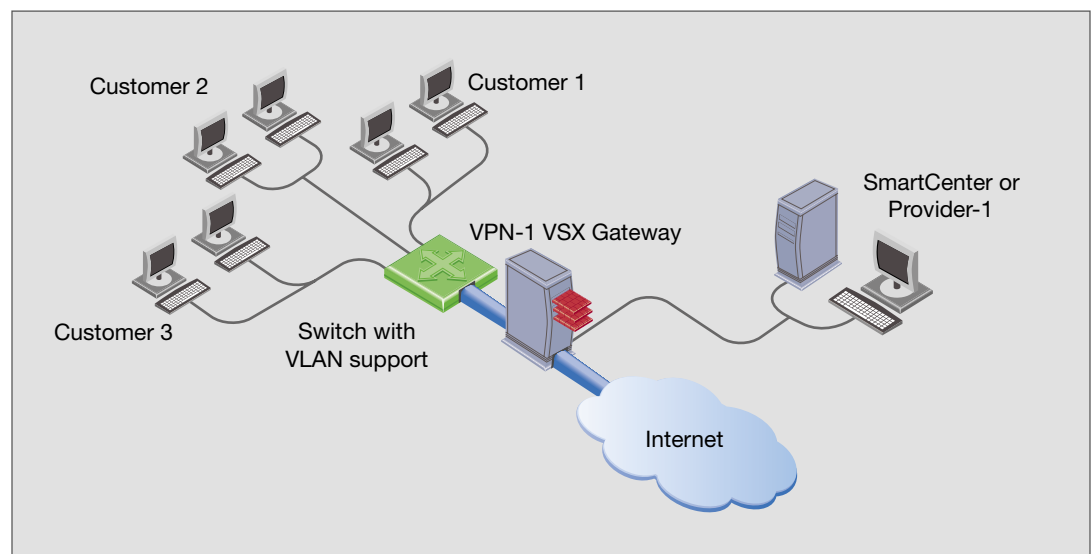
- Minimizes investment in hardware while delivering the highest levels of security
- Eliminates the need to invest in additional infrastructure for attack protection
- Enables rapid security deployment in critical environments
- Delivers non-stop wire-speed performance

YOUR CHALLENGE

Service providers and enterprises are under increasing pressure to reduce the cost of securing high-speed, mission critical environments like data centers, points-of presence (POPs) and large, segmented networks — all while providing high reliability as well as comprehensive network and application-level security. VLAN technology is often used to simplify these complex networks, but securing them effectively entails implementing access control, secure connectivity and attack protection. Common practice is to deploy separate firewall, VPN and attack protection devices in front of each network segment to achieve end-to-end security. However, implementing and maintaining large numbers of disparate solutions is expensive and time-consuming.

OUR SOLUTION

VPN-1[®] VSX NG with Application Intelligence[™] (NG with AI) uses INSPECT, the most adaptive and intelligent inspection technology, to provide an intelligent security solution specifically designed for VLAN-enabled environments such as data centers, POPs and large, segmented networks. By aggregating up to 250 comprehensive security policies on a single platform, VPN-1 VSX NG with AI minimizes hardware investment. It delivers Check Point's market-leading FireWall-1[®] on gigabit hardware platforms, and may be extended to support centralized definition, enforcement and monitoring of network and application level attack protection, remote access and desktop security. This eliminates the need to invest in and deploy multiple solutions to achieve end-to-end security. Both SmartCenter[™] and Provider-1[®] can be used to manage it, providing a centralized console to efficiently manage other Check Point gateways as well.



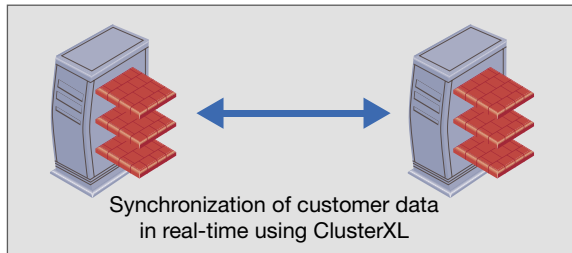
VPN-1 VSX protects up to 250 data center security domains with a single hardware platform.





SCALABLE VIRTUALIZED ARCHITECTURE

VPN-1 VSX NG with AI is comprised of multiple virtualized security domains or Virtual Systems (VS). Each VS is a complete virtualized version of a standard VPN-1 or FireWall-1 enforcement point and contains its own security policy. It also provides SmartDefense™ attack protection capabilities, delivering the highest level of security. Multiple VSs may be associated with a single physical interface on the gateway using VLAN technology, enabling customers to protect hundreds of networks using a single platform.



A cluster of VPN-1 VSX gateways delivers non-stop, wire-speed security.

WIRE-SPEED SECURITY

Performance is key in high-bandwidth environments such as data centers and POPs where hundreds of applications and users are supported. This solution can be deployed on multiple carrier-class platforms that use Check Point's SecureXL™ performance technology to deliver secure multi-gigabit throughput.

NON-STOP SECURITY

VPN-1 VSX NG with AI can be deployed in a cluster using Check Point's ClusterXL™ technology to deliver non-stop security in data center and POP environments. ClusterXL ensures that any 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 takes over without interrupting any connections.

UNPARALLELED PROTECTION

VPN-1 VSX NG with AI includes the same Stateful Inspection that market-leading FireWall-1 delivers, and supports more than 150 pre-defined applications and protocols out-of-the-box.

Examples include:

- Microsoft CI FS
- SMTP, FTP, HTTP, DNS and telnet traffic
- SOAP/XML
- Instant Messaging and Peer-to-Peer Applications
- Windows Media, RealVideo and Session Initiation Protocol (SIP)

- H.323-based services, including 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 NG with AI 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. For example, VPN-1 VSX NG with AI defends against well-known attacks such as Nimda, Code Red and Cross Site Scripting.

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 NG with AI. 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

Management of this solution 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. Using One-Click technology to add a virtual system 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. establish secure IPSec sessions with all other VPN community members.

Please visit the following URL for more information on supported platforms

http://www.checkpoint.com/products/supported_platforms/platforms_apint.html

Supported Platforms

- Check Point SecurePlatform
- Crossbeam X40/X80/X45
- Nortel Alteon Firewall 5114