Check Point SOFTWARE TECHNOLOGIES LTD.

VPN-1 UTM Edge

Secure remote connectivity with unmatched scalability

YOUR CHALLENGE

You need to establish secure and scalable communication with your organization's remote offices—such as retail outlets, branch and satellite offices, and broadband teleworkers—with limited IT staff. You need cost-effective, reliable, and flexible security gateways that integrate into your infrastructure and protect against increasingly sophisticated Internet attacks.

OUR SOLUTION

VPN-1® UTM Edge™ unified threat management (UTM) appliances provide enterprises with secure connectivity for their remote sites and are available in both wired and wireless models. By combining market-leading antivirus, firewall, intrusion prevention, and VPN technologies in a single solution, VPN-1 UTM Edge appliances ensure that remote sites stay as secure as corporate sites. Also, security management is simplified for large remote site deployments with SMART™ (Security Management Architecture) management solutions from Check Point.

RELIABLE SECURITY FOR THE NETWORK EDGE

Based on the same technologies relied upon by Fortune 500 companies, VPN-1 UTM Edge appliances provide robust security and connectivity. They secure all popular Internet services with Check Point-patented Stateful Inspection and Application Intelligence™ technologies. These Check Point solutions also support more than 150 predefined applications, protocols, and services out-of-the-box, including instant messaging, multimedia services, peer-to-peer (P2P) applications, Voice over Internet Protocol (VoIP), and Web applications. The appliances include 802.1x port-based authentication, enabling organizations to control network access at branch offices based on endpoint security policy compliance and user access privileges.

Preemptive defenses against attacks

VPN-1 UTM Edge appliances include SmartDefense™, Check Point's integrated intrusion prevention technology, to provide preemptive network- and application-layer security for remote sites. This ensures that remote sites are protected from DDoS and DoS assaults, viruses, worms, and other known and unknown attacks. SmartDefense prevents viruses and worms from entering the network and minimizes the need to invest in standalone intrusion prevention systems (IPS) at the edge of the network. SmartDefense Services protects against new threats by providing real-time defense updates and configuration advisories.

PRODUCT DESCRIPTION

VPN-1® UTM Edge™ appliances provide enterprises with secure connectivity for their remote sites. By combining market-leading antivirus, firewall, intrusion prevention, and VPN technologies in a single solution, VPN-1 UTM Edge appliances ensure remote sites stay as secure as corporate sites. Security management is simplified for large remote site deployments with Provider-1® or SmartCenter™.

PRODUCT FEATURES

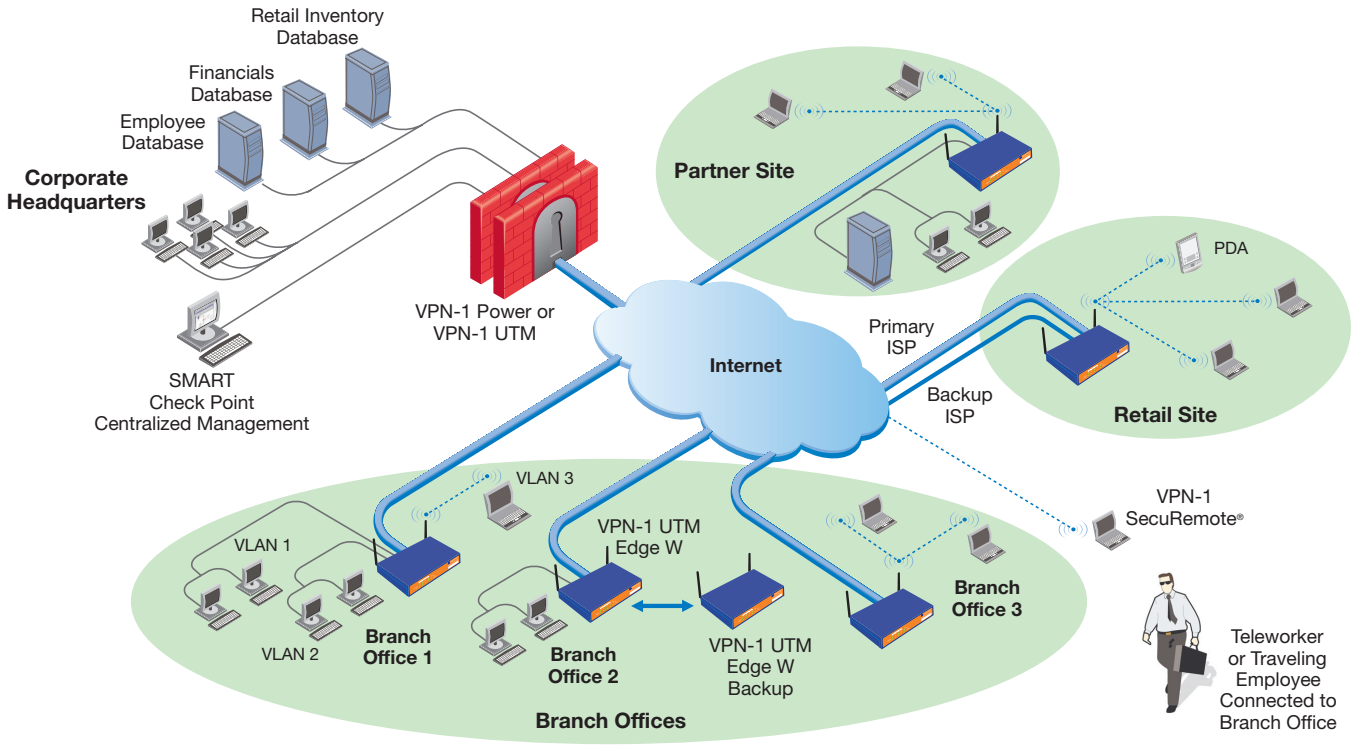
- Integrated antivirus, firewall, intrusion prevention, and VPN
- Centralized, large-scale management
- Comprehensive high availability support out-of-the-box
- Wireless LAN support

PRODUCT BENEFITS

- Provides robust security and connectivity
- Simplifies WLAN deployment and management
- Reduces network downtime at remote sites

NGX™

The NGX platform delivers a unified security architecture for Check Point.



VPN-1 UTM Edge appliances can provide enterprise-level integrated firewall and wired and wireless VPN security solutions for remote sites, branch offices, and partner sites.

Integrated gateway antivirus for in-depth defense

These appliances come equipped with integrated antivirus protection at the gateway to provide an extra layer of defense against viruses and worms hidden in emails, executables, or other files before they can enter the network. This streaming antivirus accommodates any size file with no effect on network performance. With SmartDefense Services and antivirus services subscription, remote sites can automatically receive antivirus signature updates, configuration advisories, and real-time security updates.

REMOTE SITE CONNECTIVITY

With corporations turning to virtual private networks (VPNs) to link remote offices for information access or VoIP, VPN-1 UTM Edge appliances ensure communications privacy with IPSec VPN functionality that offers strong encryption and authentication. And they can easily be added to existing VPNs.

Dynamic networks, easy deployment

For large organizations with complex networks, VPN-1 UTM Edge appliances support Open Shortest Path First (OSPF) dynamic routing. Dynamic routing enables route-based VPNs—a simpler method of defining site-to-site VPNs. Route-based VPNs make encryption decisions based on routing tables, providing flexibility in ever-changing networks.

Integrated ADSL modem

VPN-1 UTM Edge appliances are also available with integrated, high-speed ADSL modems, eliminating the need for external ADSL modems and providing administrators with simple deployment options. Support is offered for the latest ADSL standards, including ADSL v2/2+, and is available with Annex A and Annex B standards. Integrated ADSL is available for both wired and wireless appliances.

SMART MANAGEMENT

Provider-1® or SmartCenter™ can centrally manage VPN-1 UTM Edge appliances, reducing management costs for remote offices. These management products allow you to centrally define a security policy across your entire network—internal security, main sites, remote sites, SSL VPNs—all via SmartDashboard™, the central console for managing Check Point security solutions. This unified security architecture reduces the complexity of security audits by providing a single place for all security information.

With centralized profile-based management, SmartLSM™ enables administrators to define a single security profile and apply it simultaneously to thousands of VPN-1 UTM Edge appliances.

Provider-1 addresses the requirements of organizations that must manage multiple policies within their environments—such as large global enterprises or service providers. For enterprise network operations centers, it can simplify a complex security policy by segmenting it into manageable subpolicies for functional, geographic, or other groupings. For service providers, it consolidates and centralizes management for thousands of customers.

Centrally managed software updates

SmartUpdate™—available with SmartCenter Power—helps centrally manage software upgrades and licenses by automating delivery and installation of security for remote sites. This provides greater control and efficiency over distributed security architectures while dramatically decreasing maintenance costs of managing global security installations. SmartUpdate is also available as an optional module.

High availability

VPN-1 UTM Edge appliances support ISP redundancy to ensure persistent connectivity. DMZ ports may be used as secondary WAN ports, and automatic failover is supported across two gateways. Dialup backup is also supported as a cost-effective feature that provides either a primary or a secondary Internet connection if the primary broadband connection goes down. With support for USB modems, offices can also fail over to cellular connections.

Integrated Quality of Service

QoS is important for remote sites where business-critical traffic, such as VoIP or VPN traffic, is competing with noncritical traffic over a single ISP connection. VPN-1 UTM Edge appliances include comprehensive traffic management that offers weighted priorities, guarantees, and limits. Weighted priorities allocate bandwidth according to relative merit as defined by business goals, guarantees allocate minimum bandwidth levels to traffic that requires certain service levels at all times, and limits set bandwidth restrictions for noncritical network applications.

SUPERIOR WIRELESS PERFORMANCE

VPN-1 UTM Edge W appliances support multiple security protocols, including 802.1x, IPSec over WLAN, RADIUS, WEP, and WPA2 authentication. They also have dedicated WLAN interfaces from which administrators can set specific security rules for WLAN segments. This protects wireless interfaces by granting access only to authorized users, preventing hackers from attacking corporate applications or resources. In addition, the wireless interface can be segmented into as many as four virtual access points, each with separate security policies and encryption methods.

Hot spot support

VPN-1 UTM Edge appliances can be used to create guest access networks by setting up hot-spot networks. Administrators can easily require Web-based user authentication or terms-of-use approval prior to providing network access. This enables convenient, yet controlled access for guest users, without compromising corporate resources.

Wireless roaming

The Wireless Distribution System (WDS) links available from VPN-1 UTM Edge W appliances allow wireless clients to seamlessly attach to other VPN-1 UTM Edge wireless devices and standards-based access points without changing the client IP address. The access points can be interconnected by WDS links or by traditional wired Ethernet connections. WDS links can also be used to create loop-free topologies, such as stars or trees of access points, and redundant topologies, such as loops or meshes of linked access points, with bridge mode and Spanning Tree Protocol.

Wireless Multimedia Quality of Service

VPN-1 UTM Edge W appliances are the only remote office solutions that support Wireless Multimedia QoS, which prioritizes multiple types of traffic flow from different applications—such as audio, video, and voice—under various environmental and traffic conditions. It ensures that time-sensitive traffic is transmitted with minimum delay and at expected performance levels.

VPN-1 UTM EDGE APPLIANCE SPECIFICATIONS

	X8/W8	X16/W16	X32/W32	XU/WU
Size				
Total users	8	16	32	Unlimited
Interfaces				
Four-port 10/100 LAN switch	✔	✔	✔	✔
10/100 WAN port	✔	✔	✔	✔
10/100 DMZ/WAN2 port	✔	✔	✔	✔
Serial port	✔	✔	✔	✔
Optional ADSL modem	✔	✔	✔	✔
Firewall and security features				
Performance	80 Mbps	80 Mbps	80 Mbps	150 Mbps
Concurrent connections	8,000	8,000	8,000	8,000
Stateful Inspection firewall	✔	✔	✔	✔
SmartDefense	✔	✔	✔	✔
Application Intelligence	✔	✔	✔	✔
Port-based and tag-based VLAN support	✔	✔	✔	✔
Denial of Service (DoS) protection	✔	✔	✔	✔
Anti-spoofing	✔	✔	✔	✔
Gateway antivirus				
Integrated antivirus support	✔	✔	✔	✔
Supported protocols	FTP, IMAP, NBT, NUR, POP3, SMTP, UDP, and user-defined TCP ports			
On-the-fly decompression	✔	✔	✔	✔
Centralized email antivirus	POP3, SMTP			
VPN				
Performance (3DES)	20 Mbps	20 Mbps	20 Mbps	30 Mbps
Site-to-site IPSec VPN gateway	✔	✔	✔	✔
Remote access IPSec VPN client	✔	✔	✔	✔
Remote access VPN gateway	1 user	10 users	15 users	25 users

Continued on page 4

Remote access from internal networks	✔	✔	✔	✔
VPN-1 SecuRemote client licenses	Included	Included	Included	Included
MS, 3DES, DES encryption	✔	✔	✔	✔
IPSec NAT traversal	✔	✔	✔	✔
Hardware random number generator	✔	✔	✔	✔
Networking				
WAN access protocols	DHCP, PPPoE, PPTP, static IP, Telstra			
Static NAT	✔	✔	✔	✔
Hide NAT	✔	✔	✔	✔
DHCP client, relay, and server	✔	✔	✔	✔
Dead Internet connection detection	✔	✔	✔	✔
OSPF dynamic routing	✔	✔	✔	✔
Bandwidth management (QoS)	✔	✔	✔	✔
Wireless roaming	✔	✔	✔	✔
USB modem support	✔	✔	✔	✔
Bridge mode	✔	✔	✔	✔
High availability				
Gateway high availability-ready	✔	✔	✔	✔
Supports backup VPN gateway at another site (MEP)	✔	✔	✔	✔
Supports backup ISP (broadband)	✔	✔	✔	✔
Supports dial backup (requires external modem)	✔	✔	✔	✔
Automatic failover	✔	✔	✔	✔
VPN user and gateway authentication				
Site-to-site	Check Point Internal Certification Authority (Diffie-Hellman 1,024-bit PKI) digital certificates, preshared secrets, or X.509 digital certificates			
Remote access (to VPN-1 Power)	LDAP, MS ActiveDirectory, RADIUS, RSA SecurID, TACACS, XAUTH			
Remote access (to VPN-1 UTM Edge W)	Preshared secret or RADIUS			
Certificate generation for remote access	✔	✔	✔	✔
Centralized management support				
Management software	Provider-1, SmartCenter, SmartCenter Power/SmartLSM, SmartCenter UTM, SMP			
Software updates	SmartUpdate			
Reporting and monitoring	Eventia Reporter, SmartView Monitor, SmartViewTracker, Syslog			
Local Web-based management				
Installation wizard	✔	✔	✔	✔
Firewall wizard	✔	✔	✔	✔
VPN wizard	✔	✔	✔	✔
Local logs	✔	✔	✔	✔
HTTPS remote access	✔	✔	✔	✔
Additional management options				
CLI via SSH	✔	✔	✔	✔
CLI via serial port	✔	✔	✔	✔
SNMP support	✔	✔	✔	✔
Other hardware specifications				
Dimensions H x W x L	1.2 x 8 x 4.8 inches (3.0 x 20.3 x 12.2 cm)			
Weight	1.8 lbs (0.82 kg)			
Power	100-240 VAC, 50-60 Hz			
Regulatory compliance	FCC Part 15 Class B, CE			
Warranty	One-year hardware			

	W8	W16	W32	WU
Wireless LAN				
Wireless protocols	IEEE 802.11b, 802.11g, Super G*			
Wireless security	802.1x, IPSec over Wireless, MAC address filtering, WEP, WPA, WPA2, WPA-PSK			
Wireless range (regular mode)	Up to 100 meters indoors/greater than 300 meters outdoors			
Wireless range (extended range mode)	Up to 300 meters indoors/greater than 1 kilometer outdoors**			
Multiple SSIDs	✔	✔	✔	✔
Dual diversity antennas	✔	✔	✔	✔
Wireless Multimedia QoS	✔	✔	✔	✔
Hot spot mode	✔	✔	✔	✔

*Super G and XR modes require Super G- and XR-enabled wireless network adapters.
**Environmental factors may lower actual range.

February 20, 2007 P/N 502346

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
www.checkpoint.com

Check Point® SOFTWARE TECHNOLOGIES LTD.