

VPN-1 UTM

Next generation unified threat management

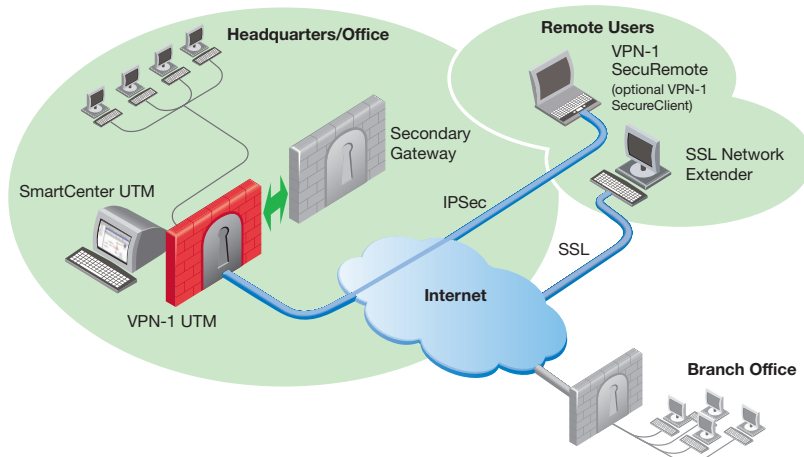
YOUR CHALLENGE

With constantly changing threats and new security challenges emerging daily, you require a solution that can keep your corporate networks safe. Faced with an increasing number of security threats, but with limited resources to address them, you require a simple, all-in-one security solution that provides the highest levels of security.

OUR SOLUTION

VPN-1® UTM™ is a unified threat management software solution that scales for enterprises of all sizes, simplifying security deployments by consolidating proven security functions within a single solution. It combines firewall, intrusion prevention, antivirus, anti-spyware, Web application firewall, VoIP security, instant messaging (IM) and peer-to-peer (P2P) blocking, Web filtering, as well as secure site-to-site and remote access connectivity in a fully integrated and easy-to-manage solution. Using the same proven Check Point security technologies that secure the Fortune 100, VPN-1 UTM gives customers a fully integrated security solution that they can rely on. Check Point's SmartCenter™ management interface, based on Check Point's NGX unified management platform, gives administrators centralized control of all security components across the entire network, reducing management overhead and complexity.

VPN-1 UTM is supported by SmartDefense Services, which maintain the most current preemptive security for the Check Point security infrastructure. To help you stay ahead of emerging threats and attacks, SmartDefense Services provide real-time updates and configuration advisories for defenses and security policies.



VPN-1 UTM delivers proven unified threat management including flexible remote access and reliable site-to-site connectivity.

PRODUCT DESCRIPTION

VPN-1® UTM™ is a unified threat management software solution that scales for enterprises of all sizes, simplifying security deployments by consolidating proven security functions within a single solution.

PRODUCT FEATURES

- Integrated firewall, intrusion prevention, antivirus, anti-spyware, Web application firewall, VoIP security, IM/P2P blocking, Web filtering, as well as secure site-to-site and remote access connectivity
- Fully centralized management including policies, updates, monitoring, and reporting
- Critical security updates and advisories provided by SmartDefense™ Services

PRODUCT BENEFITS

- Provides peace of mind with proven technologies trusted by the Fortune 100
- Protects networks, systems, and users from multiple types of Internet threats
- Ensures confidentiality by securing remote access and site-to-site communications
- Streamlines security deployment and administration
- Protects against emerging threats with SmartDefense Services



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

PROVEN UNIFIED THREAT MANAGEMENT

VPN-1 UTM actively protects organizations from known and unknown network- and application-layer attacks. By integrating proven firewall, intrusion prevention, antivirus, anti-spyware, and VPN into a single solution, VPN-1 UTM simplifies security and eliminates the need for many standalone security solutions. Similar to other Check Point solutions, VPN-1 UTM offers extensibility with a wide range of add-on components such as Web-application firewall and endpoint security modules.

Protection for business-critical applications

VPN-1 UTM examines more than 150 predefined applications, services, and protocols out-of-the-box, ensuring that the vast majority of applications used by businesses are free of threats when entering the network. Examples include:

- Voice over IP—with many companies rushing to adopt VoIP applications to lower telecommunications costs, VPN-1 UTM offers comprehensive VoIP protocol support to secure critical business communications
- Instant messaging and P2P applications—these are common attack vectors for worms, viruses, and spyware. VPN-1 UTM provides security for these applications by inspecting their content or preventing them from entering the corporate network

Gateway antivirus, worm protection, and anti-spyware

Worms and other attacks often enter the network undetected inside attachments to emails or files downloaded by users, automatically attacking all nearby computers once opened. At the same time, spyware has evolved to become one of the highest-profile IT threats to infrastructure and bandwidth. VPN-1 UTM includes gateway antivirus combined with Check Point's SmartDefense™ technology to provide antivirus and anti-spyware protection at the gateway. Antivirus scanning includes the ability to scan email (SMTP and POP3), Web (HTTP), and FTP traffic in real time for possible threats disguised inside legitimate content.

Web application firewall

Web Intelligence™, an optional component of VPN-1 UTM, provides integrated protection for Web applications against common hacking attacks such as SQL injection, cross-site scripting, and directory traversal. Included in Web Intelligence is the patent-pending Malicious Code Protector™, a revolutionary technology that detects and blocks buffer overflow attacks and malicious executables that target Web servers. Web Intelligence stops both known and unknown attacks, offering preemptive attack protection.

Web filtering

Inappropriate Web surfing can introduce security threats into your organization, as well as add risk from increased legal liability, lost productivity, and compliance issues. VPN-1 UTM software integrates best-of-breed Web filtering based on an extensive database of threat categories and associated URLs. This enables you to define an acceptable use policy for your organization and protect it from threats such as spyware and viruses, as well as new risks from inappropriate Web content.

Up-to-date protections

To maintain a preemptive security environment and ensure networks stay safe from new attacks, optional SmartDefense Services provide ongoing and automatic updates to defenses, policies, and other security elements. Organizations may have a central server download updates and automatically distribute them to remote locations or have each VPN-1 UTM gateway check independently at regular, preset intervals based on the security policy.

SITE-TO-SITE CONNECTIVITY AND REMOTE ACCESS

VPN-1 UTM delivers both IPSec and SSL VPN functionality to provide a simple and flexible way to connect remote sites and users. SSL Network Extender™, an add-on for VPN-1 UTM, delivers browser-based VPN access for Web- and other IP-based network applications providing an efficient, cost-effective remote access solution. VPN-1 UTM supports a wide range of VPN clients for businesses requiring IPSec or other client-based solutions including:

VPN-1 SecuRemote®—included with VPN-1 UTM, encrypts and authenticates data to protect against eavesdropping and data tampering

VPN-1 SecureClient™—extends VPN-1 SecuRemote features with a centrally managed personal firewall and advanced management capabilities

Microsoft L2TP VPN clients—for Microsoft users, VPN-1 UTM can provide secure remote access using a Microsoft Windows L2TP VPN client

Out-of-the-box strong authentication

Organizations that want to implement strong authentication out-of-the-box can use Check Point One-Click Certificates. With an integrated Internal Certificate Authority included with VPN-1 UTM, X.509 digital certificates can be issued to VPN-1 UTM gateways and remote-access users. One-Click Certificates provide industry-standard, two-factor authentication without the complexity and expense of PKI systems.

One-Click VPNs

By defining VPN communities with One-Click VPN, organizations can set the security parameters for an entire VPN, including site-to-site and remote access—in a single step. Your security administrators simply define all the VPN-1 UTM endpoints in a community, and VPNs are automatically enabled among all gateways or between a gateway and your remote users. As new sites are added to the community, they automatically inherit the appropriate properties and can immediately establish secure IPSec sessions with the rest of the VPN community.

Data privacy

In today's regulatory environment, data privacy is paramount. VPN-1 UTM applies the strongest encryption algorithms available for data in transit, protecting against privacy breaches. These include:

- Advanced Encryption Standard 128-256 bit
- Triple DES 56-168 bit
- Secure Sockets Layer

INTEGRATED ENDPOINT SECURITY

Remote users and partners may log on from home computers or other unsecured devices—devices outside the control of the IT department—to access email, applications, and other corporate resources. To ensure remote computers do not represent a threat, VPN-1 UTM checks for worms, keystroke loggers, and other malicious software before it allows them access to the network. It also ensures that remote users are following correct security policies, such as having up-to-date antivirus software and a personal firewall by integrating Check Point Integrity™ Clientless Security, an optional module, into VPN-1 UTM gateways.

CENTRALIZED MANAGEMENT ACROSS ALL SITES

VPN-1 UTM comes with SmartCenter, part of Check Point's SMART (Security Management Architecture) portfolio of solutions. SmartCenter offers the ability to centrally manage VPN-1 UTM gateways, as well as other Check Point products such as VPN-1 UTM Edge™ appliances. It centrally stores and distributes the security policy to the entire security infrastructure, eliminating the need to maintain each site and corresponding gateway separately. This approach greatly

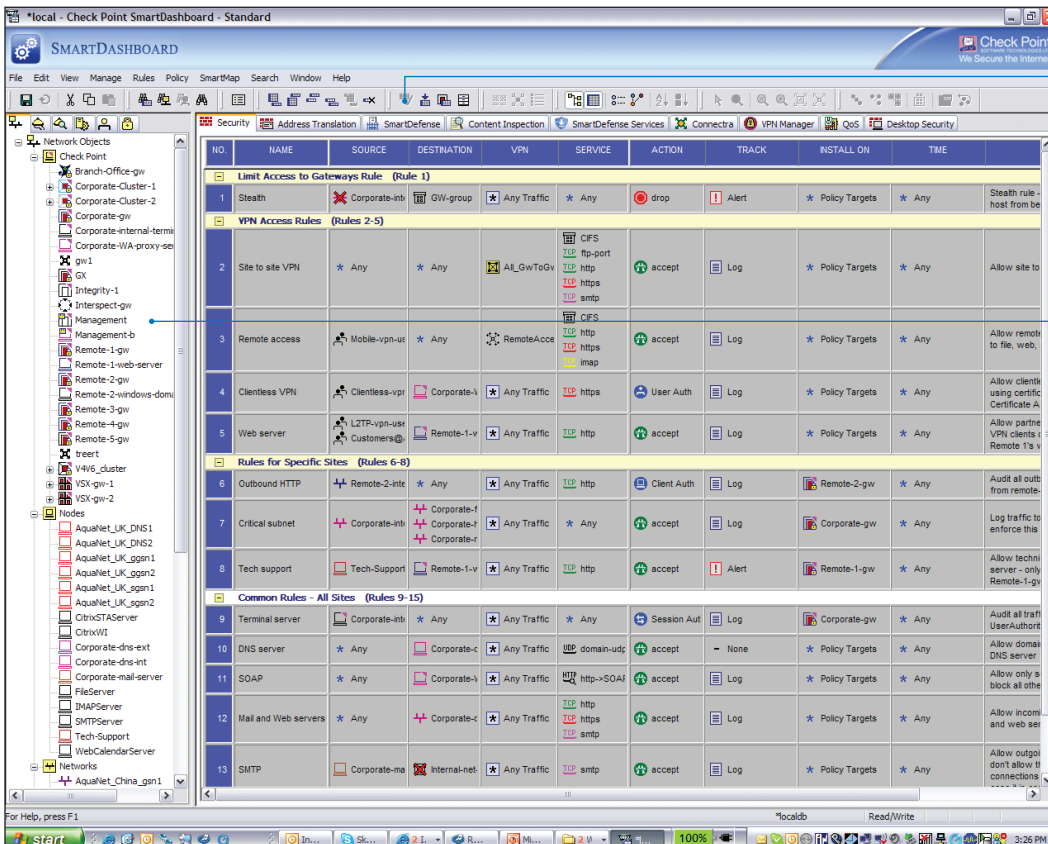
reduces administrative burden and errors and ensures consistency across the entire network. Administrators can use SmartDashboard™, the simple user interface for SmartCenter, to define and manage multiple elements of a security policy: firewall security, VPNs, network address translation, Quality of Service (QoS), and VPN client security.

AROUND-THE-CLOCK BUSINESS CONTINUITY

VPN-1 UTM is High-Availability ready to ensure that access to company resources is reliable. Multiple gateways may be deployed in a cluster to guarantee around-the-clock network availability. If the designated primary gateway becomes unreachable, all connections are seamlessly redirected to the remaining cluster members. Also, near linear performance gains are achieved when additional gateways are added to the cluster. In addition, a High-Availability interface enables traffic to be routed to a secondary interface or ISP link if the primary interface becomes unavailable. Ongoing connections are maintained during failover.

Support for VPN QoS

FloodGate-1®, an optional VPN-1 UTM module, shapes VPN traffic by assigning priority to business-critical applications and users. It delivers optimized performance, enabling customers to migrate business traffic from expensive leased lines to Internet VPNs.



All security policies and updates are easily managed across all sites.

All network objects—users, hosts, and more—are easily viewable and managed.

The SmartDashboard management interface provides centralized management of security across all sites.

Continued on page 4

Superior performance and deployment

VPN-1 UTM supports a range of deployment options to deliver a solution that best fits the performance needs for networks of any size:

- “Secured by Check Point” appliances come with preinstalled VPN-1 UTM software
- SecurePlatform™, included on the Check Point solution CD, installs a customized, hardened operating system and Check Point software in less than 10 minutes

For a list of recommended platforms, visit us online at www.checkpoint.com/products/choice/platforms.html.

ADDITIONAL CAPABILITIES

VPN-1 UTM supports a number of different enforcement modules and add-ons:

Additional VPN-1 UTM gateways secure and connect additional branch offices.

High-availability-ready VPN-1 UTM gateways can be added to an existing gateway for greater availability and resilience.

Performance accelerator cards are plug-and-play PCI add-in cards that improve the performance of existing VPN-1 UTM gateways.

VPN-1 SecureServer™ provides protection for individual application servers and secures confidential client-server communications.

ClusterXL® distributes traffic between clusters of gateways to provide performance scalability.

FloodGate-1 provides policy-based Quality of Service to optimize network performance by assigning priority to business-critical applications and end users.

SSL Network Extender™ provides full network-level access over the Web through enhanced SSL VPN capabilities.

SmartMap™ allows security managers to validate the integrity of their security by providing a detailed, graphical map of an organization's security deployment.

SmartUpdate™ delivers centralized software and license management for Check Point products to ensure that a consistent security policy is enforced throughout the enterprise network.

SmartDirectory enables VPN-1 UTM to integrate with one or more LDAP-compliant directory servers.

SmartView Monitor™ enables powerful performance analysis by presenting graphical views of end-to-end performance metrics such as bandwidth, round-trip time, and packet loss.

SmartCenter Plus extends SmartCenter with SmartMap, SmartUpdate, SmartDirectory, SmartView Monitor, and SmartPortal—a Web-based tool to access and view the security policy through a browser.

Eventia Reporter™ is an optimal reporting system that delivers in-depth network security activity and event information from Check Point log data.

UserAuthority® provides integrated Web security, single sign-on, and identity management for e-business applications.

Web Intelligence provides Web application firewall technology for Check Point products.

SYSTEM REQUIREMENTS

VPN-1 UTM gateways and SmartCenter	
Platforms	Check Point SecurePlatform, SecurePlatform Pro, and Nokia IPSO
Disk space	4 GB
Memory	256 MB (512 MB recommended)
SmartConsole	
Platforms	Solaris, Windows 2000/2003/XP/ME/98
Disk space	100 MB
Memory	256 MB
Remote access clients*	
Platforms	Windows 2000/XP/2003/Pocket PC 2003 2nd Edition/Handheld PC 2000, Macintosh, and Linux
Disk space	20 MB
Memory	64 MB

*VPN-1 SecuRemote, VPN-1 SecureClient, and Integrity SecureClient

For detailed information on supported platforms and system requirements, please refer to http://www.checkpoint.com/products/supported_platforms/platforms_appint.html.

©2003–2007 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, Confidence Indexing, ConnectControl, Connectra, Connectra Accelerator Card, Cooperative Enforcement, Cooperative Security Alliance, CoSa, DefenseNet, Dynamic Shielding Architecture, Eventia, Eventia Analyzer, Eventia Reporter, Eventia Suite, Firewall-1, Firewall-1 GX, Firewall-1 SecureServer, FloodGate-1, Hacker ID, Hybrid Detection Engine, IMsecure, INSPECT, INSPECTXL, Integrity, Integrity Clientless Security, Integrity SecureClient, InterSpect, IPS-1, 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, Sentivist, 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. ZoneAlarm is a Check Point Software Technologies, Inc. Company. 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.

February 26, 2007 P/N 502345

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.