



VPN-1 MASS

Scalable secure access for next-generation carrier networks

YOUR CHALLENGE

As their networks evolve, your customers are placing greater demands on you to provide anywhere, anytime access to information. To support the new, evolving communications technologies needed to meet these demands takes more than moving from 3G networks to a converged IP infrastructure. It means providing the same robustness and reliability shown in today's network while building a flexible, adaptable architecture to support still-evolving technologies for tomorrow. Most important, it requires building advanced security into a converged IP infrastructure to enable these new technologies without jeopardizing end-customer information, because convergence means your protected carrier-core network will now be exposed to the public Internet and the threats that it carries.

OUR SOLUTION

VPN-1® MASS (Multi-Access Security Solution) delivers the foundation of secure fixed/mobile convergence (FMC) for carriers—enabling them to deliver advanced communications products to their customers without compromising network security. Supporting 3G Wireless Interworking (3G I-WLAN), Unlicensed Mobile Access (UMA)—also known as Generic Access Network (GAN)—and traditional VPN remote access, VPN-1 MASS scales to provide remote access for up to 100,000 secure voice channels and massive numbers of data connections.

SCALABLE COMMUNICATIONS FOR CUSTOMER SERVICES

The advent of dual-mode phones—offering both cellular and wireless LAN access—means you have had to adopt the 3G I-WLAN or UMA set of standards within your network. VPN-1 MASS supports both sets of standards, giving you the flexibility to design an architecture that best suits your network.

For 3G I-WLAN networks, VPN-1 MASS supports both the GSM/UMTS and CDMA2000 standards and can inspect tunneled traffic to stop fraudulent or malicious activity. VPN-1 MASS is able to inspect major Voice over Internet Protocol (VoIP) protocols, including H.323, SIP, and others. Similarly, UMA signaling traffic is inspected to protect carrier network integrity.

PRODUCT DESCRIPTION

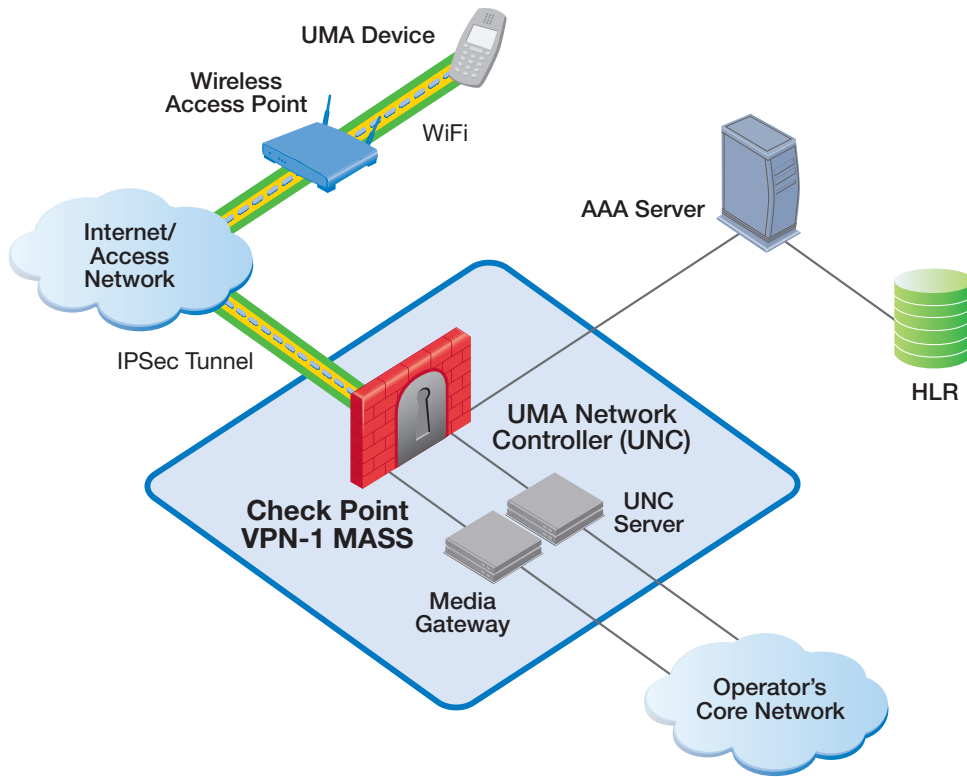
VPN-1® MASS provides a secure-access solution for carriers deploying next-generation infrastructures such as Unlicensed Mobile Access (UMA).

PRODUCT FEATURES

- Integrated security and VPN for UMA access
- High availability

PRODUCT BENEFITS

- Enables additional access services for carrier customers
- Ensures security of carrier networks against attack
- Easily integrates with UMA networks



VPN-1 MASS is commonly deployed as a security gateway in front of a UMA network controller (UNC). In a UMA deployment, it utilizes an Authentication, Authorization, and Accounting (AAA) server to authenticate users through RADIUS as a front end to the core-network authentication infrastructure.

Supported 3G standards
3GPP TS 23.234: 3G I-WLAN system description
3GPP TS 29.234: 3G I-WLAN Stage 3
3GPP TS 33.234: 3G I-WLAN Security
3GPP TS 43.318: GAN Stage 2
3GPP TS 44.318: GAN Stage 3
3GPP2 X.P0028-200: 3GPP2 I-WLAN
Supported interfaces
UMA: Wm (using RADIUS), Up (security level only)
I-WLAN: Wm (using RADIUS), Wu

VPN-1 MASS provides communications confidentiality through Check Point’s IPsec virtual private network (VPN) technologies—including the latest standards such as EAP-SIM and IKEv2. Carriers can choose from a variety of clients to provide strong encryption between client devices and a carrier network. VPN-1 MASS has been tested for interoperability with numerous handsets from leading device vendors.

Advanced security

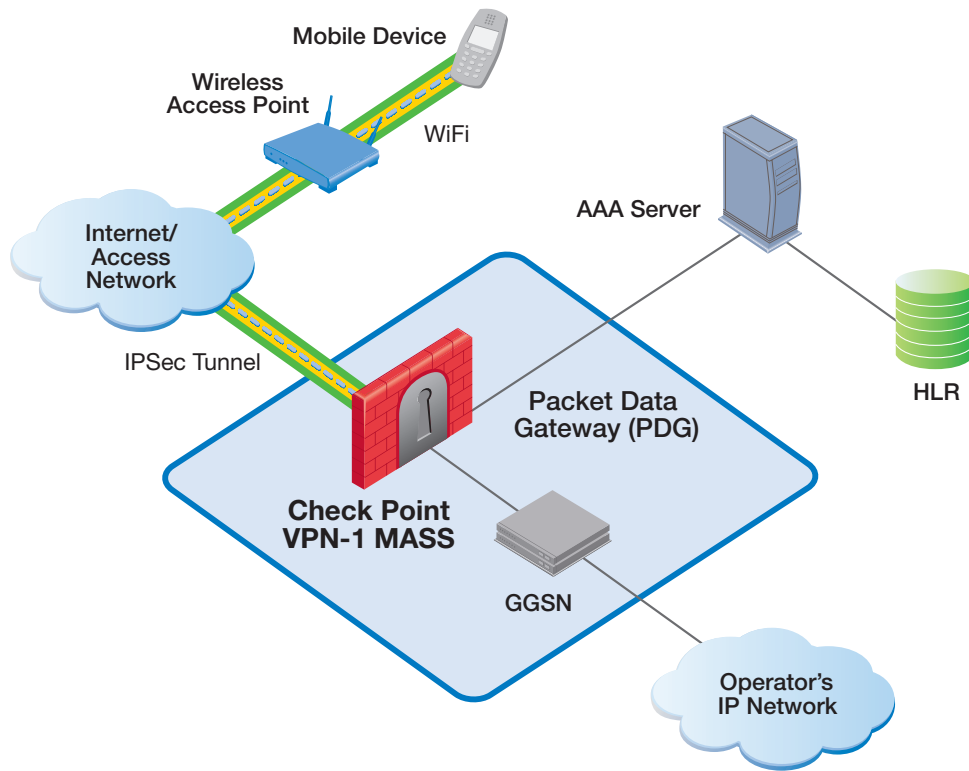
Opening up the network to the Internet introduces a number of risks to the carrier, but VPN-1 MASS mitigates those risks by incorporating the advanced security technologies found in the VPN-1 family. Check Point’s patented Stateful Inspection technology, coupled with its Application Intelligence™ intrusion prevention, provides a proven defense against the threats found on the Internet as well as shielding the carrier network from client-based attacks.

Ensuring reliability and performance

With support for high availability, VPN-1 MASS helps ensure that downtime and poor performance do not affect carrier reputations. Carriers can deploy multiple VPN-1 MASS security gateways to provide instantaneous failover for connections, with no need for IPsec renegotiations that would lower call quality.

Flexible integration options

VPN-1 MASS is an open solution that integrates with third-party FMC and VoIP solutions. This frees carriers to design best-of-breed solutions, maximizing services offered to customers. VPN-1 MASS also integrates with carrier backend systems.



VPN-1 MASS, along with a GGSN, is part of the Packet Data Gateway (PDG) solution in a 3GPP I-WLAN network. In addition, VPN-1 MASS uses a AAA server to authenticate incoming client devices.

Specifications	
Supported platforms	Please view latest platform support on http://www.checkpoint.com
AAA (Authentication, Authorization, and Accounting) supported authentication methods	RFC 2865: RADIUS RFC 2866: RADIUS Accounting RFC 3579: RADIUS Support for EAP RFC 4186: EAP-SIM Authentication RFC 4187: EAP-AKA Authentication
Supported IPsec standards	RFC 2451: CBC in ESP RFC 3602: AES-XCBC in ESP RFC 3947: IKE NAT traversal RFC 3948: IPsec UDP Encapsulation RFC 4301: IPsec Security Architecture RFC 4303: Encapsulating Security Payload (ESP) RFC 4305: Cryptographic algorithms for ESP and AH RFC 4306: IKE version 2 RFC 4307: Cryptographic algorithms for IKEv2 RFC 4308: Cryptographic suites for IPsec and IKE RFC 4434: AES-XCBC for IKE
Certificate support and handling	X.509 v3 certificates, including generation of certificates and support for third-party certificates
Next-generation infrastructure support	UMA, 3G I-WLAN

Continued on page 4

About Check Point Software

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, personal firewall, 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 product line is the highest rated personal computer security suite, composed of award-winning endpoint security solutions that protect millions of PCs from hackers, spyware, and data 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 more than 350 leading companies. Check Point solutions are sold, integrated, and serviced by a network of more than 2,200 Check Point partners in 88 countries, 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>

©2003–2007 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 22, 2007 P/N 502434

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.