



VPN-1 UTM

Next Generation Unified Threat Management

Overview

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. Based on the same Check Point technologies that secure the Fortune 500, VPN-1 UTM delivers uncompromising security while streamlining deployment and administration. VPN-1 UTM offers a complete set of security features including firewall, intrusion prevention, antivirus, anti-spyware, messaging security including anti-spam, 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.

Features

- Proven application control and attack protection
- Gateway antivirus, anti-spyware
- Comprehensive messaging security with anti-spam
- Web Filtering
- Virtual Security

Proven application control and attack protection

VPN-1 UTM includes the most proven firewall and can examine hundreds of applications, protocols, and services out-of-the-box. Integrated SmartDefense IPS utilizes signature- and protocol-anomaly-based intrusion prevention to protect business-critical services like FTP, HTTP, and VoIP from known and unknown attacks. Similarly, VPN-1 UTM can block non-business applications like IM and P2P.

Gateway antivirus, anti-spyware

Gateway antivirus and anti-spyware are core components of VPN-1 UTM, complementing desktop endpoint security. VPN-1 UTM uses an up-to-date list of antivirus and antispyware signatures and anomaly-based protection to stop viruses and other malware at the gateway. To check for threats hidden inside legitimate content, real-time antivirus scans are performed on POP3, SMTP, FTP, and HTTP services.

Comprehensive messaging security with anti-spam

Messaging Security from Check Point provides comprehensive protection for an organization's messaging infrastructure. The multidimensional approach protects the email infrastructure, provides highly accurate spam protection, and defends organizations from a wide variety of virus and malware threats within email.

IP reputation anti-spam	Blocks spam and malware at the connection level by checking the sender's reputation against a dynamic database of known malicious IP addresses
-------------------------	--

Content-based anti-spam	Protects against advanced forms of spam, including image-based and foreign-language spam, using pattern based detection
Block/allow list anti-spam	Utilizes block or allow lists to deny obvious email offenders and allow trusted senders Protects against a wide range of viruses and malware, including scans of message content and attachments
Mail Antivirus	Protects against a wide range of viruses and malware, including scans of message content and attachments
Zero-hour outbreak protection	Defends against new spam and malware outbreaks by using advanced pattern matching and distribution analysis engine
SmartDefense email IPS	Protects against a broad range of threats, including DoS and buffer overflow attacks, that target the messaging infrastructure itself

Web Filtering

VPN-1 UTM stops inappropriate Web surfing with best-of-breed Web filtering that covers 20-million-plus URLs, so you can define an online acceptable-use policy for your organization.

Simple site-to-site connectivity

With VPN-1 UTM, you can simplify the setup of site-to-site VPNs and remote access. Manual setup of node-to-node VPN tunnels and security for an entire VPN is replaced by a One-Click process, where new sites and remote users are added automatically.

Secure, flexible remote access

VPN-1 UTM gateways can connect employees and business partners to your trusted network through flexible IPsec or SSL-based remote access, working seamlessly with a variety of VPN agents

Integrated SmartCenter management

VPN-1 UTM gateways come with integrated SmartCenter management, offering the ability to centrally manage multiple appliances and other Check Point products from a single console. It centrally stores and distributes security policy for the entire infrastructure, eliminating the need to maintain each site and gateway separately, reducing administrative burden and errors, ensuring consistency across the network. Through the intuitive SmartDashboard, administrators define and manage elements of a security policy: firewall security, network address translation, Quality of Service (QoS), VPN agent security, and VPNs.

Virtual Security

VPN-1 UTM can be deployed as VPN-1 VE, enabling you to secure your virtual environments with the same level of protection as the rest of the network. Certified by VMware, it enables you to quickly provision security within virtual systems without requiring complex network reconfiguration.

For companies desiring to consolidate multiple security gateways on a single hardware platform, VPN-1 Power VSX enables you to virtualize up to 250 VPN-1 gateways on a single, secure virtual platform.

Specifications

Protections Details

Firewall	
Protocol/Application support	Secures more than 200 applications and protocols
VoIP Protection	Sip, H.323, MGCP, and SIP with NAT support
Instant Messaging Control	MSN, Yahoo, ICQ, and Skype (including over HTTP and SSL)
Peer-to-peer Blocking	Kazaa, GNUTella, BitTorrent, eMule, IRC (including over HTTP)
Network Address Translation	Static/hide NAT support with manual or automatic rules
IPSec VPN	
Encryption Support	AES 128-256 bit, 3DES 56-168 bit
Authentication Methods	Password, RADIUS, TACACS, X.509, SecurID
Certificate Authority	Integrated X.509 certificate authority
VPN communities	Automatically sets up site-to-site connections as objects are created
Topology Support	Star and mesh
Route-based VPN	Utilizes Virtual Tunnel Interfaces, numbered/unnumbered interfaces
VPN Client	Check Point Endpoint Security, VPN-1 SecureClient, VPN-1 SecuRemote
SSL VPN	
SSL-based remote access	Fully integrated SSL VPN gateway provides on-demand SSL-based access
SSL-based endpoint scanning	Scans endpoint for compliance/malware prior to admission to the network
Intrusion Prevention	
Network-layer protection	Blocks attacks such as DoS, Port Scanning, IP/ICMP/TCP related
Application-layer protection	Blocks attacks such as DNS cache poisoning, FTP bounce, improper commands and more
Detection Methods	Signature-based and protocol anomaly
Antivirus / Anti-spyware	
Antivirus protection	Protects HTTP, FTP, POP3, and SMTP protocols
Anti-spyware blocks	Pattern-based spyware blocking at the gateway

Updates	Centralized, daily updates
Web Filtering	
URL database	20 million-plus URLs covering 3 billion-plus Web pages
Language support	More than 70 languages spanning 200 countries
Updates	Centralized, daily updates (100,000-plus new sites a week)
Messaging Security	
Email IPS	SMTP, POP3, and IMAP attack protection
Pattern-based anti-spam	Detects spam based on dynamic database of signatures
IP reputation checking	Blocks spam and malware by sender
Signature-based antivirus	First layer of protection from viruses and malware
Zero-hour outbreak protection	Complements signature-based protection to block new outbreaks
Block/allow lists	Provides granular control over specific domains and users
Networking	
Virtualization	Can be deployed as certified virtual appliance in VMware environments
VLANs	256
DHCP Support	SecurePlatform™ DHCP server and Relay
Layer-2 bridge support	Transparently integrates into existing network
ISP Redundancy	Protocol-based, source/destination and port route decisions
Performance and Availability	
Failover recovery	Optional ClusterXL for Active/standby bridge mode for instantaneous failover
Load balancing	Optional ClusterXL
Quality of Service	FloodGate-1 for granular QoS
ISP Redundancy	Automatically reroutes traffic to second interface
Traffic Acceleration	Optional SecureXL accelerates security decisions

HARDWARE SPECIFICATIONS

Platforms	Check Point Secure Platform, Microsoft Windows Server, Sun Solaris, RedHat Enterprise Linux
Free Disk Space	Windows and Linux : 300 MB Solaris: 128 MB SecurePlatform: 10 GB (OS Inclusive)
Memory	Windows and Linux: 256 MB (512 MB Recommended) Solaris: 128 MB SecurePlatform: 256 MB (512 MB Recommended)

For detailed information on supported platforms and system requirements, please refer to [this page](#).

Support

Check Point offers many technical support options for customers. These range from the Standard support plan that provides telephone assistance during normal business hours with next-day shipment of replacement appliances, to the Premium support plan providing 24/7 assistance with same day replacement shipment, up to the Premium+4H plan that provides a qualified engineer on-site within four hours to resolve any appliance-related issues. For additional information, please visit the [Support Programs](#) section of our website.

Direct Enterprise Support

Support Service	Software Subscription	Standard	Premium	Diamond (On Top Of Premium)
Basic SLA	N/A	5x9 Business Day	7 x 24 Every Day	7 x 24 Every Day
Latest Hot Fixes & Service Packs	Yes	Yes	Yes	Yes
Major Upgrades & Enhancements	Yes	Yes	Yes	Yes
Support Focal Point	N/A	Desks Support Engineer	Premium Support Engineer	Designated Diamond Engineer
Unlimited Service Requests	N/A	Yes	Yes	Yes
Committed Response time to Severity-1 issues	N/A	30 Minutes	30 Minutes	30 Minutes
Committed Response time to Severity 2,3 & 4 issues	N/A	4 Hours	Sev 2 – 2 Hours Sev 3 & 4 – 4 Hours	Sev 2 – 2 Hours Sev 3 & 4 – 4 Hours
Access to Check Point Products Forums	Read	Full Access	Full Access	Full Access

Access to Online Support Knowledgebase	N/A	Advanced	Expert	Expert
Appliance Support*				
Default Appliance support (if the appliance is covered within the account rate)	1st Year Warranty	Standard	Premium	Premium
Return Material Authorization (RMA) determination	TAC	TAC	TAC	Customer
RMA Shipment Method	Within 7 Business Days from faulty unit return	Same business day shipment ¹	Next Flight Out / Express Delivery (when applicable) or Same Business Day Shipment ³	Next Flight Out / Express Delivery (when applicable) or Same Business Day Shipment ³
Onsite RMA Shipment Method (must be purchased in addition to the regular program SLA)	N/A	5 x 8 x NBD Delivery and basic installation of replacement hardware by a certified engineer ²	7 x 24 x 4H Delivery and basic installation of replacement hardware by a certified engineer	7 x 24 x 4H Delivery and basic installation of replacement hardware by a certified engineer

1. For Return Material Authorization determination completed by 15:00 regional hub time; otherwise shipment will occur next business day with delivery target extended by one day
2. Available in over 250 locations world wide.
3. Next Flight Out / Express Delivery is available in the European Union and mainland US. Appliances are shipped during normal business hours and may arrive during off hours or next business day until 9AM.

* Learn more about [Check Point Security Appliances Support Programs](#)

Collaborative Enterprise Support

Support Service	Co - Standard	Co - Premium	Co - MSP
TAC access by the certified support partner / MSP	7 x 24 Every Day	7 x 24 Every Day	7 x 24 Every Day
Latest Hot Fixes & Service Packs	Yes	Yes	Yes
Major Upgrades & Enhancements	Yes	Yes	Yes
Support Focal Point (to partner/ MSP)	Desks Support Engineer	Premium Support Engineer	Premium Support Engineer

Unlimited Service Requests	Yes	Yes	Yes
Committed Response time to Severity-1 issues	Indirect 30 Minutes	Direct 30 Minutes	Direct 30 Minutes
Committed Response time to Severity 2,3 & 4 issues	4 Hours	Sev 2 - 2 Hours Sev 3 & 4 - 4 Hours	Sev 2 - 2 Hours Sev 3 & 4 - 4 Hours
Direct Access to Check Point TAC for Severity-1 issues	No	Yes 7 x 24	Yes 7 x 24
Access to Check Point Products Forums	Full Access	Full Access	Full Access
Access to Online Support Knowledgebase	Advanced	Expert	Expert
Appliance Support*			
Default Appliance support (if the appliance is covered within the account rate)	Co - Standard	Co - Premium	Co - Premium
Return Material Authorization (RMA) determination	TAC	TAC	TAC
RMA Shipment Method	Same business day shipment ¹	Next Flight Out / Express Delivery (when applicable) or Same Business Day Shipment ³	Next Flight Out / Express Delivery (when applicable) or Same Business Day Shipment ³
Onsite RMA Shipment Method (must be purchased in addition to the regular program SLA)	5 x 8 x NBD Delivery and basic installation of replacement hardware by a certified engineer ²	7 x 24 x 4H Delivery and basic installation of replacement hardware by a certified engineer	7 x 24 x 4H Delivery and basic installation of replacement hardware by a certified engineer

¹ For Return Material Authorization determination completed by 15:00 regional hub time; otherwise shipment will occur next business day with delivery target extended by one day.

² Available in over 250 locations world wide.

³ Next Flight Out / Express Delivery is available in the European Union and mainland US. Appliances are shipped during normal business hours and may arrive during off hours or next business day until 9AM.

* UTM-1 Edge RMA is shipped Next Business Day for all SLAs.

* Learn more about [Check Point Security Appliances Support Programs](#)

©2010 Check Point Software Technologies Ltd. All rights reserved.