



### PRODUCT DESCRIPTION

Check Point Safe@Office® UTM appliances deliver comprehensive, enterprise-class security in a turnkey desktop appliance—ideal for protecting small and medium-size businesses and providing secure remote access to corporate resources

# Safe@Office UTM Appliances

## YOUR CHALLENGE

In order to operate effectively and enable growth, today's small and medium-size businesses must provide employees and third parties with access to critical resources and information. However, even a small data breach can expose growing companies to crippling lawsuits, penalties and loss of reputation. As hacking techniques and malware improve, the threat of data loss compels companies to further restrict access to sensitive data. With limited IT budgets and resources, small businesses need an inexpensive, yet comprehensive solution to provide secure access to critical resources from anywhere, while minimizing the risk of a data breach.

## OUR SOLUTION

Check Point Safe@Office® UTM appliances deliver proven, best-in-class security with reduced cost and complexity—right out of the box! Small businesses can quickly and easily deploy comprehensive protection, including firewall, IPS and anti-malware, starting at just \$299. Robust performance, intuitive management and advanced wireless options provide unmatched value in a simple, all-in-one solution.

### Security

#### Best-in-class Integrated Firewall and IPS

Safe@Office UTM appliances include the industry's most proven firewall technology, based on the same Check Point technologies that secure the Fortune 100. Comprehensive network access control (NAC) allows blocking of unwanted applications such as IM and P2P, while an advanced intrusion prevention system (IPS) ensures protection of remote sites from both known and unknown threats, such as Denial-of-Service, post scans and buffer overflows.

#### Secure Connectivity

IPSec VPN connectivity secures communications between site-to-site and remote locations. Support for multiple VPN clients—such as Check Point Endpoint Connect, SecureClient, SecuRemote and L2TP—offers flexibility for users.

#### Anti-malware and Messaging Security

Malware protection is integrated at the gateway, blocking worms and viruses before they enter the network. On-the-fly decompression of unlimited file sizes enables thorough scanning. Check Point Messaging Security blocks spam and provides comprehensive protection for an organizations' messaging infrastructure.

### PRODUCT FEATURES

- Best-in-class integrated firewall and intrusion prevention system (IPS)
- Anti-malware, messaging security, Web filtering and network access control (NAC)
- Wizard-based management including preset security rules, automatic updates, monitoring and reporting
- Seamless 802.11n WiFi and 3G wireless connectivity
- Comprehensive traffic management parameters guarantee quality-of-service (QoS)

### PRODUCT BENEFITS

- Comprehensive, enterprise-class security for SMBs in a single appliance
- Gigabit firewall performance starting at \$750
- High-availability options ensure that security functions keep pace with business-critical applications
- Quick and easy deployment with minimal IT resources



<b>IP reputation anti-spam</b>	Checks the sender's reputation against a dynamic database of known-bad IP addresses, blocking spam and malware at the connection level.
<b>Content-based anti-spam</b>	Blocks known spam by comparing a 'fingerprint' of each incoming email with a dynamic database containing millions of known spam signatures.
<b>Block/allow list anti-spam</b>	Blocks email offenders while allowing trusted senders. Can block or allow entire domains.
<b>Mail antivirus</b>	Blocks worms and viruses at the gateway. Supports standard email protocols (POP3, IMAP, and SMTP), including Web-based email.
<b>IPS email server protection</b>	Protects against a broad range of threats, including denial-of-service attacks that target the messaging infrastructure itself.

### Web Filtering

Best-of-breed URL filtering services allow companies to define Web access policies. Access to potentially malicious Web sites containing spyware and viruses, as well as inappropriate Web content can be blocked.

### Network Access Control (NAC)

802.1X port-based authentication allows NAC based on user privileges and policy compliance at branch offices. Built-in support for the extended authentication protocol (EAP) enables WPA Enterprise and 802.1X access control without an external RADIUS server. This makes NAC easier to use, even in small networks.

### Networking

#### High-Performance Networking

Safe@Office appliances are full-fledged network routers that include a LAN switch, a dedicated DMZ and a WAN port (Ethernet or ADSL). Static and dynamic routing options are available for complete interoperability.

Safe@Office 1000N Series appliances come equipped with superior networking and security capabilities including state-of-the-art hardware acceleration and 6-1Gbps Ethernet ports.

#### Secure Hot Spot Support

Administrators can easily enable guest access to networks by creating Web-based secure hot spots. User authentication and/or terms-of-use can be required before granting access to corporate resources.

#### High Availability

High-availability options ensure that security functions keep pace with business-critical applications and other network activity. Safe@Office UTM appliances support WAN redundancy and load balancing to ensure persistent connectivity and service availability. Should the broadband connection become unavailable, dialup support can provide a backup Internet connection.

#### Quality-of-Service (QoS)

Comprehensive traffic management parameters such as weighted priorities, bandwidth guarantees and bandwidth limits can guarantee QoS for business-critical or latency-sensitive traffic over a single Internet connection. Wireless Multimedia QoS allows companies to prioritize traffic from multiple audio, video and voice applications.

### Wireless Roaming

By using the Wireless Distribution System (WDS) capability, the network can be extended by interconnecting two or more Safe@Office wireless appliances. This allows wireless clients (e.g., laptops, PDAs) to connect seamlessly to the wireless network without the need to change IP addresses.

### Management

#### Quick and Easy Setup

A simple Web-based management interface allows administrators to secure a small business in minutes. The setup wizard allows the selection of a preset firewall policy, or the creation of a custom security policy. Security rules can be easily modified with a variety of remote management options.

#### Network Monitoring

Safe@Office logs information on attempted attacks and displays it in a color-coded report which includes the IP addresses from which the attacks originated. A "Who Is" utility allows administrators to identify an IP address owner, providing Internet "caller ID" capability. Built-in traffic monitoring and packet capture tools enable monitoring and control of inbound/outbound traffic for efficient bandwidth utilization.

#### Redundant Internet Connectivity

Safe@Office 1000N and 1000NW appliances also provide complete support for PSTN and ISDN, as well as a wide variety of 3G cellular modems. Out-of-bound dial-in is also supported, to ensure access to the appliance even during Internet connection failures.

#### Updates

Optional subscription-based services provide continuous software and antivirus updates, including URL filtering services, periodic security reports, and anti-spam and dynamic DNS services.

### Hardware Options

#### Secure Wireless Connectivity

Safe@Office 1000N Series appliances integrate a WiFi access point (802.11b/g/n) supporting multiple security protocols, including 802.1x, IPsec over WLAN, RADIUS, WEP, WPA and WPA2 authentication. They also have dedicated WLAN interfaces from which you can set specific security rules for WLAN segments. In addition, the wireless interface can be segmented into as many as four virtual access points, each with separate security policies and encryption methods.




Safe@Office 500W Series appliances integrate a WLAN access point that supports the Super-G and Extended Range (XR) standard, enhancing the range and network speeds of the wireless access point. Additionally, wireless networks can be segmented into multiple virtual access points, each with different security policies and encryption settings. Remote users are authenticated using a variety of authentication standards including WPA2.

#### Integrated ADSL Modem

Safe@Office appliances are available with integrated, high-speed ADSL modems, eliminating the need for external ADSL modems and providing administrators with simple deployment options. The latest standards, including ADSL v2/2+, Annex A and Annex B are supported.



**SPECIFICATIONS**

			
Safe@Office Series	Safe@Office 500 Safe@Office 500W	Safe@Office 500 ADSL Safe@Office 500W ADSL	Safe@Office 1000N Safe@Office 1000NW
Security Functionality	Firewall, VPN, Intrusion Prevention, Antivirus, Anti-spam, URL Filtering		
On-board Management	Yes		
Wireless LAN	802.11 b/g: 500W, 500W ADSL 802.11 b/g/n: 1000NW		
Support for 3G Modem	-	-	Yes
Software Edition	Embedded NGX 8.1		
Ethernet Ports	6: 10/100	5: 10/100	6: 10/100/1000
Firewall Throughput	190 Mbps		1,000 Mbps
VPN Throughput	35 Mbps		200 Mbps
Concurrent Sessions	8,000		60,000
VLANS	32		64
Enclosure	Desktop		
Dimensions (W x H x D)	20 x 3.1 x 12.8 cm (7.87 x 1.22 x 5.04 in.)		
Operating Temperature	0° to 35° C (32° to 95° F)		
Operating Humidity	10%-90%, non-condensing		
Power Input	100/240V, 50/60Hz		

**CONTACT CHECK POINT**

**Worldwide Headquarters**

5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | 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