



Firewall & Compliance Check

Controls in and outbound traffic and ensures policy compliance with centralized management from a single console

Firewall & Compliance Check

YOUR CHALLENGE

Attackers are getting smarter and smarter by finding new ways to maliciously compromise endpoint systems. The best corporate firewalls cannot stop all malicious inbound and outbound traffic, especially when a user is not always working within a corporate network. Providing endpoints with firewalls can be a logistical nightmare due to the scale of deployment, lack of centralized control, and logging capabilities.

PRODUCT DESCRIPTION

The Check Point Firewall & Compliance Check Software Blade protects endpoints by controlling inbound and outbound traffic and ensuring policy compliance, with centralized management from a single console. Desktop Firewall policies protect endpoint systems from unauthorized access. Integrated stealth technology makes endpoints invisible to attackers. This software blade is easily managed by unified Endpoint Security Management.

OUR SOLUTION

Check Point Firewall & Compliance Check guards against network worms, malware, unauthorized access, and attacks from suspicious sources. Unique to Check Point Firewall, stealth technology makes endpoint systems invisible to attackers. Finally, providing unified security options in a single management console and server make enforcement and monitoring of incidences easier.

Desktop Firewall

- Regulate inbound and outbound traffic at the endpoint systems to prevent infections by worms, malware, unwanted traffic, and access to the endpoint from unauthorized people

Compliance Check

- Scan endpoint systems for corporate security policy compliance.
- Automatic and transparent remediation for non-compliant endpoints
- Ability to restrict non-compliant endpoints from accessing sensitive corporate resources
- Enforce a dedicated endpoint security policy (across all endpoint software blades) to non-compliant endpoints.

PRODUCT FEATURES

- The desktop firewall protects the integrity of endpoints by regulating inbound and outbound traffic.
- Compliance scanning ensures endpoint systems are compliant with corporate security policy.
- Central Management enables policy enforcement and logging.

PRODUCT BENEFITS

- Control inbound and outbound traffic for malware and intrusion protection along with policy compliance.
- Centrally definable traffic control, security levels and stealth technology.
- Verify that endpoints meet the organizational security policy. Prevent non-compliant devices to access sensitive resource, and transparently remediate such devices.
- Integration with Check Point Software Blade Architecture for a single-console, centrally-managed endpoint solution.



Central Management

- Centrally managed by the Endpoint Policy Management Software Blade, enabling central policy administration, enforcement, and logging from a single, user-friendly console.

Integrated into Check Point Software Blade Architecture

- The Desktop Firewall & Compliance Check Software Blade is fully integrated into the Software Blade architecture, saving time and reducing costs by allowing customers to quickly expand security protection while keeping a single client and simple user experience to meet changing requirements.
- Additional Endpoint Security Software Blades: Antimalware and Program Control, WebCheck Browser Virtualization, Media Encryption and Port Protection, Full Disk Encryption, and Remote Access VPN.

SPECIFICATIONS

Compliance Check

Verify Programs	Verify if a certain program is running or not running on the endpoint device
Verify Files	Verify if a certain file exists or does not exist on the endpoint device
Verify Registry Keys	Verify if a specific registry key and value is set or not set on the device
Verify Anti Malware Solution and Virus Signature Age	Supports the following vendors: Check Point, Symantec, McAfee, Trend Micro, Kaspersky, Nod32, AVG, Avast, Sophos, Panda CA, Inoculate IT engine, BitDefender, MS Forefront
Restricted policy	Ability to enforce a dedicated security policy for non-compliant endpoints
Remediation	Ability to automatically remediate non-compliant endpoints

Firewall Configuration Options

- Inbound Firewall
- Outbound Firewall
- Stealth Mode

Client Platform Support

- Microsoft Windows 8 Enterprise and Professional (32 & 64-bit)
- Microsoft Windows 7 Enterprise, Professional, Ultimate editions (32 & 64-bit) and SP1
- Microsoft Windows Vista (32 & 64-bit)
- Microsoft Windows XP Pro (32-bit, SP2 and later)

Client Language Support

- English
- Japanese
- French
- Italian
- German
- Chinese (simplified)
- Spanish
- Russian

Management Platform

See Endpoint Policy Management Software Blade

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

959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233 | www.checkpoint.com