CHECK POINT
ANTI-SPAM SOFTWARE BLADE

CHECK POINT ANTI-SPAM SOFTWARE BLADE

Comprehensive protection for messaging infrastructures

Product Benefits

- Increase employee productivity with industry-leading spam and phishing catch rates, coupled with near-zero false positives
- Reduce hardware with our high performance, low maintenance anti-spam solution
- Simply enable anti-spam on your existing Check Point gateway and you are protected
- We keep up with new spam attack tactics and detection management so you don’t have to.

Product Features

- IP and content reputation checks
- Zero-hour outbreak protection
- Mail antivirus
- Customizable Block/allow list
- Integrated into the Software Blade Architecture

[1] Verizon 2015 DBIR report

INSIGHTS

Email continues to be one of the most successful infection vectors for malware writers. Not only unwanted, email spam may contain malicious links or attachments that lead to significant costs and losses to an organization. Email cannot be blocked making it easy for malicious files to get through. Even security conscious users may not recognize when an email is malicious. More than one out of ten people will open an email attachment from a sender they don't know[1]. Organizations need to protect their users from this email-borne threat. Unfortunately, keeping up with the ever-changing tactics of spammers can consume valuable hardware and personnel resources.

SOLUTION

Delivering industry-leading detection performance, our Anti-Spam Software Blade allows real-time blocking of spam and phishing in any language or format with almost no false positives.

Check Point Anti-Spam technology blocks spam based on its most fundamental characteristics - mass distribution and repeating patterns. Spam and phishing outbreaks distributed via email share identifiable patterns such as sender IP addresses, embedded URLs, and combinations of characters from the subject and body of the email. Rather than relying on content scanning, our approach bases detection on:

- Email distribution patterns – senders (how many, location) and volume of the emails sent over a period of time
- Structure patterns – in the email messages and attachments

With this approach, our Anti-Spam solution is equally effective against all types of spam in any location, format, content, or language. With proven resilience, we analyze billions of emails daily in real-time, recognizing and protecting against new spam outbreaks and phishing attacks the moment they emerge.

A GLOBAL PROTECTION PLATFORM

The largest global cloud infrastructure security platform powers our Anti-Spam Software Blade. Multiple carrier-grade data centers and multiple worldwide traffic collection nodes gather billions of internet transactions daily.

HOW IT WORKS

Our Anti-Spam technology automatically analyzes collected traffic with a unique global view of outbreaks, providing accurate spam and phishing classifications.

A local cache provides spam classification to the engine, or, if not identifiable locally, via a fast query to the cloud infrastructure. The result: instant protection from new outbreaks without any lag in updates.

BLOCK/ALLOW LIST

The Anti-Spam Software Blade utilizes block or allow lists to deny obvious email offenders and allow trusted senders.

Administrators can easily create a list of IP addresses or domains that they would like to either always block or always allow. This adds a layer of granularity, explicitly allowing trusted sources and explicitly denying access to unwanted sources. Blocked IP addresses and domains appear in the summary section for the Block/Allow list in the anti-spam security management tab.

ZERO-HOUR OUTBREAK PROTECTION

Zero-hour outbreak protection defends against new spam and malware outbreaks by using a distributed analysis engine.

By analyzing large amounts of messages on a global level, it identifies outbreaks along with their corresponding messages. It then flags these message patterns as malicious, giving the Anti-Spam Software Blade the most current information about a given attack. This blocks outbreaks before a signature may be available, protecting your network in the critical early period of an attack.

MULTI-LAYER PROTECTION

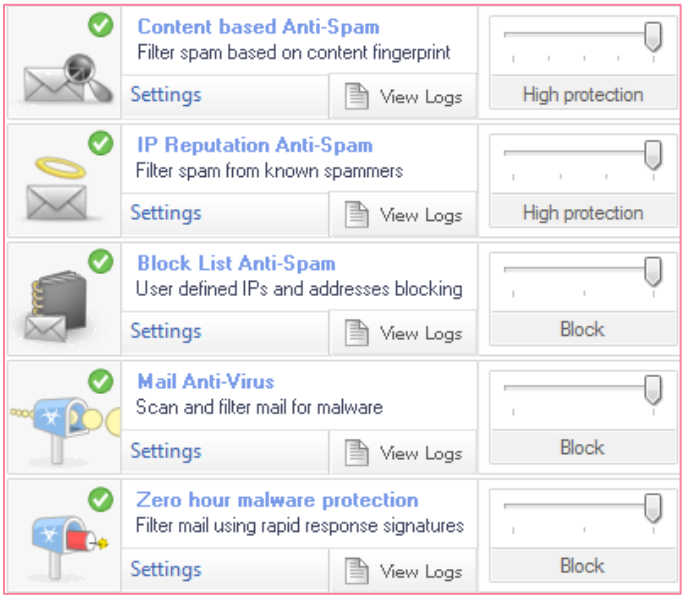
The Anti-Spam Software Blade is part of a multi-layered approach to protect your email infrastructure. Our Next Generation Threat Prevention software package includes the Anti-Spam, IPS and the Antivirus Software Blades, protecting organizations from a wide variety known and unknown threats delivered within email.

MAIL ANTIVIRUS

Beyond blocking many attacks at a sender level, the Anti-Spam Software Blade includes a highly-rated antivirus engine that scans POP3 and SMTP mail protocols. Mail antivirus scans message content and attachments to protect you from a wide range of viruses and malware.

SIMPLE CONFIGURATION

Configuration is a snap with our integrated Software Blade Architecture. Simply enable Anti-Spam on your existing Check Point gateway and you are protected by the default configuration. From there, easily customize your configuration to your liking. The Anti-Spam Overview provides a simple and informative explanation of your status.



EVALUATE ANTI-SPAM TODAY

Save time and reduce costs significantly by automatically implementing Check Point Threat Prevention technologies in your existing security infrastructure. Get started with a trial today, or learn more about the Check Point Anti-Spam Software Blade.

CONTACT US

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