CHECK POINT
INTRUSION PREVENTION SYSTEM (IPS)

Intrusion Prevention Systems detect or prevent attempts to exploit weaknesses in vulnerable systems or applications, protecting you in the race to exploit the latest breaking vulnerability. Check Point Intrusion Prevention System (IPS) provides complete, integrated, next generation firewall intrusion prevention capabilities at multi-gigabit speeds with high security effectiveness and a low false positive rate. IPS protections in our Next Generation Firewall are updated automatically. Whether the vulnerability was released years ago or today, your organization is protected.

Our defense in depth approach combines signatures, protocol validation, anomaly detection, behavioral analysis, and other methods to provide the highest levels of network IPS protection. Check Point IPS provides complete threat coverage for vulnerabilities in clients, servers, operating systems and widely available applications such as PDF readers and browsers that are the preferred targets of threat actors.

Detect and Prevent Exploits with Assurance

EFFICIENT

Our acceleration technologies let you safely enable IPS. A low false positive rate saves your staff valuable time

SECURE

Check Point IPS delivers thousands of signature and behavioral preemptive protections

UNIFIED

Enable IPS on any Check Point security gateway reducing Total Cost of Ownership

Online attacks and malware have been evolving, using sophisticated and even evasive attack methods. Check Point addresses the changing threat landscape while meeting several key operational requirements for Intrusion Prevention Systems. Check Point IPS protections include checks for protocol and behavioral anomalies which means we detect vulnerabilities in well-known protocols such as HTTP, SMTP, POP, and IMAP before an exploit is found.

Check Point IPS protects you with:

- Detection and prevention of specific known exploits, for example protection from specific CVEs
- Detection and prevention of DNS tunneling attempts indicating data leakage or evasion
- Detection and prevention of generic attack types without any pre-defined signatures
- Detection and prevention of protocol misuse which may indicate malicious activity

Preemptive Security Updates

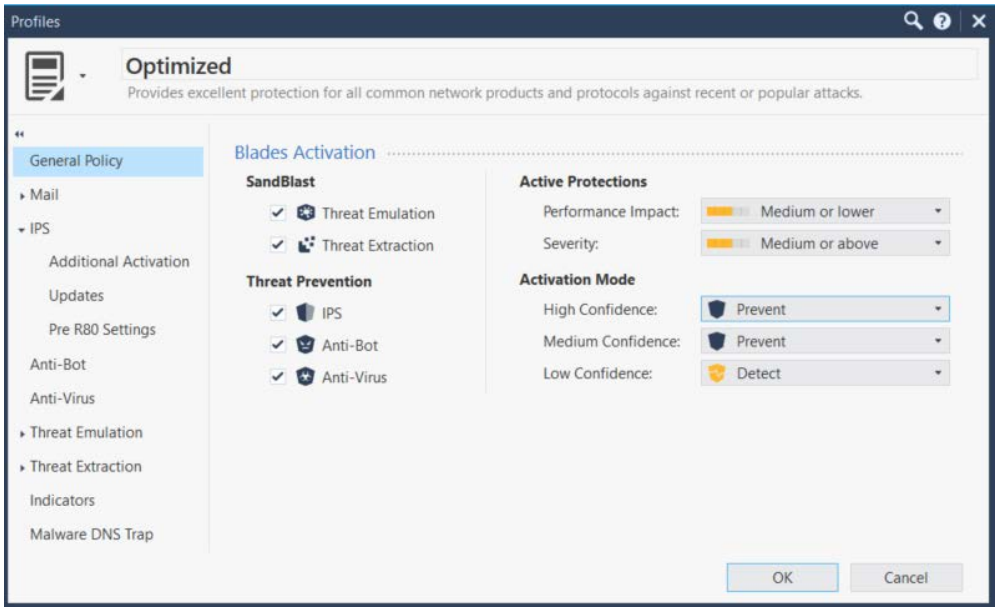
Patching is an incomplete security measure, which can leave your network open for attack. By taking a more comprehensive approach, which combines robust IPS functionality with a concerted patching strategy, network administrators can better equip themselves to handle ‘Patch Tuesdays’ and secure the network between upgrades and patches. Let your Check Point Next-Gen Firewall do the security updates for you. Virtual patching is seamless when protections are updated automatically every 2 hours on the Check Point management server and security gateways. In addition new protections are flagged for follow-up ensuring admins stay on top of any changes to their IPS policy.

PROFILES SIMPLIFY IPS MANAGEMENT

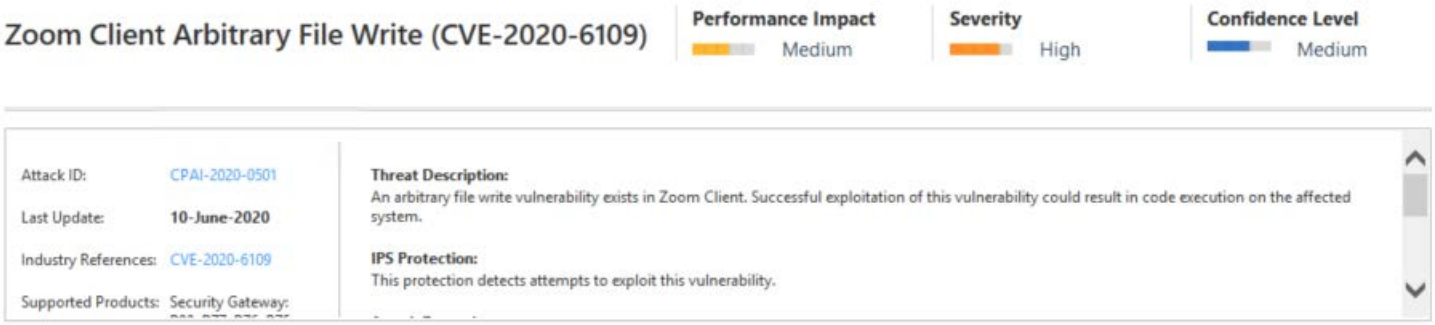
Painless Deployment

Reduce deployment time and costs by leveraging existing security infrastructure. Optional detect-only mode sets all your existing protections to only detect, but not block, traffic to allow you to evaluate your profile without risking disruption. Simply enable IPS on your existing Check Point Next Generation Firewall. IPS is included in the NGFW package. Want protection from more advanced zero-day and threats in files? Enable antivirus, Anti-bot and SandBlast (sandboxing) Zero-day protection. IPS is also included in the Next Gen Threat Prevention and the SandBlast packages.

Predefined default and recommended profile settings allows for immediate and easy out-of-the-box use with profiles tuned to optimize security or performance.



Each protection is described with 3 attributes; Severity, Confidence and Performance Impact. Protection profiles allow administrators to define signature and protection activation rules that match the security needs of their network assets.



Severity

The Common Vulnerability Scoring System is an open industry standard for assessing the severity of computer system security vulnerabilities where scores range from 0 to 10, with 10 being the most severe. Similarly Check Point assigns a severity level to each IPS protection.

Confidence Level

Some attack are less severe than others, and legitimate traffic may sometimes be mistakenly recognized as a threat, also known as a false positive. The confidence level value is an estimate of how well a protection can correctly recognize a specific attack.

Performance Impact

Some protections require the use of more resources or apply to common types of traffic, which adversely affects the performance of the gateways on which they are activated. This attribute enables better management of the performance of your NGFW.

IPS TAILORED TO YOUR NEEDS

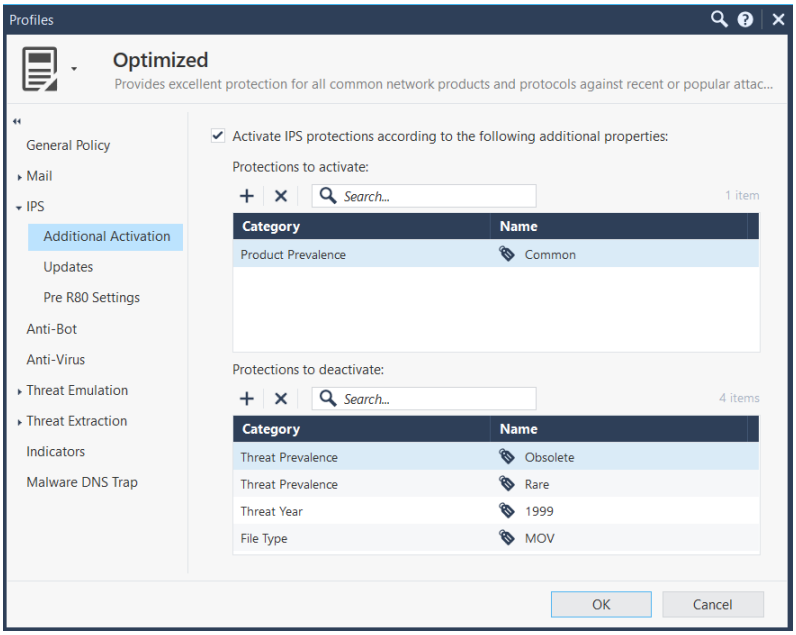
Unified Threat Management

IPS is configured and managed through a single Check Point management interface. This includes tightly integrated event management. Achieve an unmatched level of visibility to detect and prevent threats. Check Point IPS seamlessly integrates with SmartEvent enabling SOC (Security Operations Center) staff to respond to the highest priority events first, saving them time.

Track events through detailed reports and logs of what is most important to simplify threat analysis and reduce operational overhead. Customizable reports provide easy monitoring of critical security events associated with your business-critical systems. Directly from the security event, go to the associated protection, create an exception or view packet captures.

IPS Tags

In addition to severity, confidence and performance impact you can also activate and deactivate IPS protections using these attributes or tags; vendor (400+), product (600+), threat year, file type, protocol and the effect of the vulnerability such as information disclosure and DoS. This allows security administrators to create an IPS policy that better fits their environment. Profiles and protection attributes greatly simplify management of over 8,000 IPS protections. In your security logs there is a wealth of information about your organization. This includes newly installed applications that may be vulnerable. Analysis will identify these applications and you can then use an IPS tag to activate IPS protections to virtually patch any vulnerable applications found.



IPS Best Practices

SmartEvent pre-defined views reveals IPS protections in Detect mode that can safely be moved to prevent mode. Most important are the ones where a detect event occurred, but the connection was not prevented by the IPS because of the Detect setting. IPS security best practice number one is to follow up on these events.

Scalable Tbps IPS Performance

Check Point was the first to exploit the performance capabilities of industry standard multi-core processors for IPS, bringing intelligent load-balancing among cores to enable fast, fully-integrated IPS functions in one firewall. Now with Maestro Hyperscale network security, customers can distribute load across multiple Check Point firewalls in N + 1 clusters to achieve over a Terabit per second of IPS throughput. With Check Point IPS technologies, you can have confidence that your organization's network will get top performance and full functionality without compromising on security.

CONTACT US

Worldwide Headquarters | 5 Shlomo Kaplan 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: 650-628-2117 | www.checkpoint.com