NGTP, WAF, OWASP TOP 10
Reduce Risk Using Complementary Security Technologies

INSIGHTS

Bad actors have several avenues into your network. Users can be tricked into visiting malicious sites or opening malicious attachments. A more direct route is to exploit vulnerabilities in Internet-connected applications, using a variety of web-specific attacks such as SQL injection, client-side attacks, automated web bot and hacking activities. Regardless of the attack vector, a single successful exploit can set a breach in motion. Stolen user credentials and application exploits can both be leveraged to access corporate databases and other sensitive information, causing financial and reputational damage to the target, system hijacking, theft of intellectual property and downtime.

PROTECT NETWORKS AND APPLICATIONS

Check Point Next Generation Threat Prevention (NGTP) gateways and Web Application Firewalls (WAF) are complementary technologies that protect your data, users, applications and infrastructure in real-time as threats are detected. Check Point protects your networks and users with multi-layered defense and SandBlast Zero-Day Protection (sandboxing). WAFs protect your web applications from common attacks by inspecting the XML/SOAP traffic and also inspecting HTTP/HTTPS for typical attacks at layer 7 such as SQL Injections, Buffer Overflow, Cross Site Scripting (XSS), File Inclusion, Cookie Poisoning, etc.

While there is some overlap between NGTP gateways and WAFs, there are also a great number of protections unique to each solution. The two technologies complement each other. Use the security tasks in each that are suited to their strengths.

Web Application Firewalls. Best at…	Next Generation Threat Prevention Gateways. Best at…
Web Scraping Protection	Application Based Visibility and Access Control
Web Server Cloaking	Detection of Protocol Based Anomalies
Load Balancing / SSL Offloading	Full IPS Protection on ALL traffic (not just Web)
Web Traffic Baseline / Profiling	Bot/Malware and other Post Infection Detection
URL Encryption	East-West Intra VNET Application Layer Control
Web Server Vulnerability Analysis	Limiting bandwidth based on Application ID
Dedicated Application Protection	Fully integrated perimeter and network boundary control

WAF Use Case Example

An administrator wants to prevent web scraper bots from lifting web content. Threat Prevention gateways deployed in Software Defined Data Centers (SDDC) are not well suited for this kind of activity.

Threat Prevention Gateway Use Example

An administrator wants to ensure that communications between Web Application Virtual Machines (VMs) and Database VMs are legitimate SQL requests (versus malware traffic taking advantage of open SQL ports). The admin may also want to quarantine a VM or endpoint if the VM is found to be infected. A WAF is of no help under this East-West or lateral propagation scenario. Only an NGTP Gateway provides the required visibility and application control needed to quarantine this infected host.

A security best practice is to deploy Next Generation Threat Prevention and Web Application Firewalls and use the unique strengths of each product to secure your Internet-facing applications.

THREAT PREVENTION COVERAGE – OWASP 2017 TOP 10 [1]

Any discussion of practical application security technology would be amiss if it didn't include how it complimented or fits in with the Open Web Application Security Project (OWASP) Top 10. OWASP is a not-for-profit charitable organization focused on improving the security of software so that individuals and organizations worldwide can make informed decisions about software security risks. The OWASP Top Ten represents a broad consensus on the most critical software application security flaws from a variety of security experts from around the world.

The OWASP Top Ten is a list of general vulnerability classes so the level of coverage that security products provide against such vulnerabilities cannot be easily defined or measured. IPS products such as Check Point IPS usually detect well-known vulnerabilities rather than track the behavior of custom web applications which means this list and the classification of vulnerabilities into classes is not designed in the way IPS products categorize vulnerabilities. This document provides some notes regarding Check Point's protection against these vulnerability classes, focusing mainly on Check Point IPS.

	OWASP 2017 Top 10	**Check Point Protection**
A1: Injection *2013 – A1,* *2010 – A1*	Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.	IPS includes several generic protections against injection vulnerabilities: • SQL injection • LDAP injection • Command Injection • HTTP Command Injection SQL and Command Injection Attacks are blocked by looking for keywords. Keywords are traced in form fields either in GET or POST request, inside the URL or the HTTP request body. Keyword lists are preconfigured, and users only need to set the security level on HIGH/MEDIUM/LOW. When a higher security level is used, keywords that are less indicative of an attack are also examined. In addition, Check Point IPS currently offers ~250 protections against specific well-known SQL injection vulnerabilities, and ~80 more other command injection and other injection-related vulnerabilities.
A2: Broken Authentication *2013 – A2* *2010 - A3*	Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.	Organizational applications intended for internal users could protect themselves against such implementation flaws by using Check Point's authentication and Identity Awareness features, performing the authentication at the Firewall (which could in turn query an external database, such as LDAP, Windows, RADIUS, Citrix, RSA SecurID, Cisco pxGrid, etc.). In addition, Check Point IPS offers protections against some known attacks on specific servers which exploit known authentication and session management vulnerabilities.

	OWASP 2017 Top 10	Check Point Protection
A3: Sensitive Data Exposure 2013 – A6	Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.	Check Point IPS contains ~150 protections against specific vulnerabilities involving information disclosure. Applications intended for internal users can use Check Point's VPN / Remote Access features in order to enable encrypted and authenticated access to sensitive data, while not exposing it to external attackers. This can be done either by an IPsec VPN tunnel or by a clientless SSL/TLS VPN.
A4: XML External Entities (XXE) 2017 - New	Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.	Check Point IPS contains ~75 protections against known XML processor vulnerabilities in software such as Apache, Microsoft, Drupal, Oracle and Citrix.
A5: Broken Access Control Merged 2013 A4+A7	Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as access other users' accounts, view sensitive files, modify other users' data, change access rights, etc.	Organizational applications intended for internal users could control access rights to the various functionalities by using Check Point's authentication and Identity Awareness features. In addition Check Point IPS protects against Brute Force login attempts.
A6: Security Misconfiguration 2013 – A5 2010 – A6	Security misconfiguration is the most commonly seen issue. This is commonly a result of insecure default configurations, incomplete or ad hoc configurations, open cloud storage, misconfigured HTTP headers, and verbose error messages containing sensitive information. Not only must all operating systems, frameworks, libraries, and applications be securely configured, but they must be patched and upgraded in a timely fashion.	IPS offers a "Header Spoofing" feature, which allows an administrator to hide the identity of the Web server from scripts looking for vulnerable Web servers. IPS also offers protections against misconfigured applications, such as attempt to use the default credentials of some well-known applications, or attempts to use some deprecated protocols, methods, options and parameters. In addition, Web servers that are not kept up-to-date with the current security patches would still be protected against many of the vulnerabilities which these patches solve by various Check Point IPS protections.
A7: Cross Site Scripting (XSS) 2013 – A3 2010 – A2	XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.	IPS offers a generic Cross-Site scripting protection, which rejects any occurrence of HTTP request containing banned HTML tags and escape sequences that may be used for scripting, as well as ~130 XSS protections against specific vulnerabilities, which look for multiple keywords that can be used for scripting code, JavaScript and VBScript commands, event that can trigger scripting engine, and HTML attributes and tags.
A8: Insecure Deserialization 2017 - New	Insecure deserialization often leads to remote code execution. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.	Applications that are not kept up-to-date with the current security patches would still be protected against many of the vulnerabilities which these patches solve by various Check Point IPS protections.

	OWASP 2017 Top 10	Check Point Protection
A9: Using Components with Known Vulnerabilities 2013 – A9	Components, such as libraries, frameworks, and other software modules, run with the same privileges as the application. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications and APIs using components with known vulnerabilities may undermine application defenses and enable various attacks and impacts.	Network security products may only inspect the traffic that passes over the network. If the use of the vulnerable component results in unique traffic for that component, it may be identified regardless of the application that uses that component. However, if the vulnerable component is an infrastructure used in different ways by different applications, and does not result in distinct traffic that can be identified, it is outside the scope of a network security device.
A10: Insufficient Logging and Monitoring 2017 - New	Insufficient logging and monitoring, coupled with missing or ineffective integration with incident response, allows attackers to further attack systems, maintain persistence, pivot to more systems, and tamper, extract, or destroy data. Most breach studies show time to detect a breach is over 200 days, typically detected by external parties rather than internal processes or monitoring.	In addition to on-device application logs, it's important to log session data on enforcement points in a properly segmented network. Logs from Check Point NGTP gateways, endpoint and mobile security products are key to deconstructing any attack. Check Point logging tools like SmartLog and SmartEvent are essential tools for any Security Operations Center (SOC). Check Point logs include severity ratings to help your SOC staff prioritize the most important events first. We try to keep false positives to a minimum [4]. Check Point also integrates with major SIEM vendors like Splunk, ArcSight, IBM QRadar and others.

OWASP 2013 TOP 10 NOTABLES [2]

	OWASP 2013 Top 10	Check Point Protection
A8: Cross-Site Request Forgery (CSRF) 2010 – A5	A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.	IPS offers protections against several specific CSRF vulnerabilities in WordPress, Oracle, Adobe, Trend, Symantec and other products.
A10: Invalidated Redirects and Forwards 2010 – A10	Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.	IPS offers protections against several known redirection vulnerabilities in Apache, IIS, IE, Forefront, WordPress and other products.

OWASP 2010 TOP 10 NOTABLES [3]

	OWASP 2010 Top 10	Check Point Protection
A7 Insecure Cryptographic storage	Many web applications do not properly protect sensitive data, such as credit cards, SSNs, and authentication credentials, with appropriate encryption or hashing. Attackers may steal or modify such weakly protected data to conduct identity theft, credit card fraud, or other crimes.	Check Point products include built-in support for encryption protocols and provide the highest level of security and management capabilities for encryption functions, so that the burden of implementation cryptographic functionality is shifted from the Web application developer to Check Point. Organizational applications intended for internal users could use Check Point's VPN / Remote Access features in order to enable encrypted and authenticated access to sensitive data, while not exposing it to external attackers. This can be done either by an IPsec VPN tunnel or by a clientless SSL/TLS VPN. As for users' credentials for authentication performed at the Firewall, they could be stored securely on an external server (LDAP, Windows, RADIUS, Citrix, RSA SecurID, etc.) queried by the Firewall. In addition, Check Point offers Full Disk Encryption as well as other media encryption solutions to help protect sensitive data from unauthorized direct access.
A8: Failure to restrict URL Access	Many web applications check URL access rights before rendering protected links and buttons. However, applications need to perform similar access control checks each time these pages are accessed, or attackers will be able to forge URLs to access these hidden pages anyway.	Check Point's authentication and Identity Awareness features could be used to restrict access to certain URLs for specific authenticated internal users only, instead of relying only on the web application's own authentication. In addition, IPS protections such as Directory Traversal protections and Null HTTP Encoding prevent URL manipulation that could fool URL-base authorization mechanisms.
A9: Insufficient Transport Layer Protection	Applications frequently fail to authenticate, encrypt, and protect the confidentiality and integrity of sensitive network traffic. When they do, they sometimes support weak algorithms, use expired or invalid certificates, or do not use them correctly.	The Check Point Security Management Server allows the security administrator to require that certain connections must be authenticated or encrypted. Encryption and authentication could be carried out by the Firewall, including checking certificate integrity and validity and using strong and secure authentication and encryption algorithms. In addition, Check Point IPS includes many protections against vulnerabilities in SSL clients and servers and attempts to exploit vulnerabilities in the SSL protocol.

SUMMARY

The OWASP Top 10 provides a framework for prioritizing the most critical security risks to applications that organizations face today. Practical application security can be achieved using the strengths that are unique to complimentary technologies like those in Web Application Firewalls and in Check Point Next Generation Threat Prevention products. Threat agents have several attack vectors from which to launch attacks. It is as important to protect your Internet facing applications from direct threats as it is to protect them from indirect threats like that from a user compromised by a successful spear phishing attack.

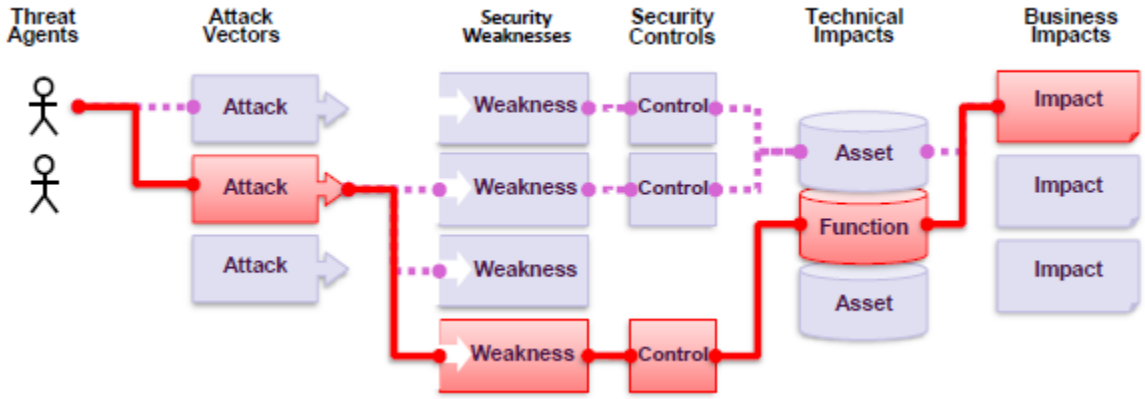

Figure 1: OWASP Top 10 - Application Security Risks [1]

"To determine the risk to your organization, you can evaluate the likelihood associated with each threat agent, attack vector, and security weakness and combine it with an estimate of the technical and business impact to your organization."

References

[1] OWASP 2017 Top 10: Retrieved from
https://www.owasp.org/images/7/72/OWASP_Top_10-2017_en.pdf
[2] OWASP 2013 Top 10: Retrieved from
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2013
[3] OWASP 2010 Top 10: Retrieved from
https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2010
[4] (Dec-20-2017), Blog: Check Point NSS BPS Test Highlights, Retrieved from
http://blog.checkpoint.com/2017/12/20/nss-recommends-check-point-advanced-threat-prevention/

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: 650-628-2117 | www.checkpoint.com

