Leveraging Machine-Learning Algorithms to Automate the Process of Security Policy Generation

The web application attack landscape is evolving quickly in conjunction with the ongoing changes around application development, hosting and maintenance. New DevOps trends and cloud migration are forcing application security teams to investigate new ways to keep up with new vulnerabilities and to manage policies across disparate hosting environments. As cyberattacks and mitigation techniques continue to evolve, enterprises need to look beyond static protections and focus more on automated and adaptive solutions in order to protect their networks and applications effectively.

A core part of Radware's security offering is to provide protection for web applications. Through its ICSA Labs certified web application firewall and its enterprise-grade Cloud WAF Service, Radware offers full web security protection including OWASP Top 10 coverage, advanced attack protection and zero-day attack protection that automatically adapts an organization's protection to evolving threats and protected assets.

Radware's WAF technology incorporates machine-learning algorithms to keep web assets secure regardless of evolving threats or changes to applications and environments.

Going Beyond Static Signature Protection

The most common protection includes a negative security model, which defines what is disallowed, while implicitly allowing everything else. Most web application security solutions leverage a negative security model that utilizes few signatures for specific and previously seen attacks. Relying solely on negative security models, as is the case with most cloud WAF services, offers only partial protection against OWASP Top 10 risks. In most of the cases different risk categories will not be covered at all.

Blocking zero-day attacks, which are previously unseen attacks, requires a different approach rather than signature-based protection. A positive security model, which defines the set of allowed types and values is required to provide a proper protection, where signature-based protection cannot fill the gap.

Yet, the use of these security models requires defining policies and rules which can sometimes be labor intensive. Radware's goal is to use automation to reduce the cost of ownership and to avoid human errors associated with such manual processes. Auto-policy generation technology introduces machine-learning capabilities for automatic rule definition and maintenance. Different methodologies may be involved with automation, where the idea is to identify the legitimate traffic to the application, and profile the application based on that traffic. Most WAF solutions, especially cloud services, do not offer any Auto-policy generation capabilities, while those that do offer such tools are focused on very specific attack categories, such as DDoS attacks.

Radware's Auto-Policy Generation Technology

As part of its WAF, Radware offers an Auto-Policy Generation mechanism that provides the best tool for automatically generating security policy for the secured web application. The Auto-Policy Generation module will automatically utilize the required security filter, create security filter rules, and switch the security filters into active mode.

These operations would normally require manual refinements. Building a security policy usually demands intensive work on the part of the administrator, while still leaving a system potentially open to attack due to human errors.

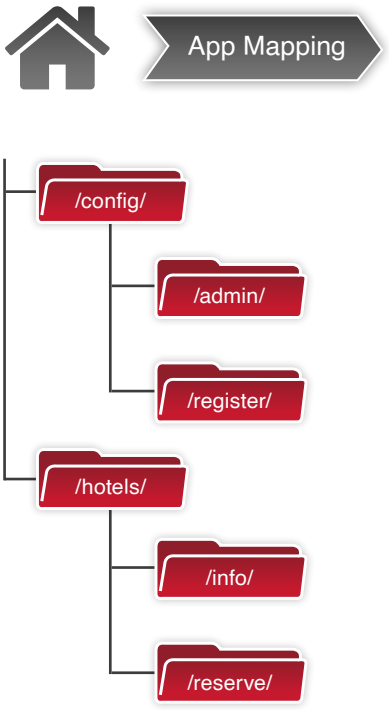
By leveraging machine-learning algorithms, Auto-Policy Generation can secure a web application automatically with limited user interaction. There are different attributes of the secured application, and the environment needs that impact the process of policy generation. The system automatically discovers the structure of a web application, while at the same time, Auto-Policy Generation sets the relevant security filters, analyzes traffic properties from the production environment, and builds a dynamic network profile for a specific site according to the Auto-Policy Generation module.

Auto-Policy Generation creates rules for different security filters. For example, when enabled, the Parameters security filter rules are automatically generated by the Auto-Policy Generation module. When enabled, the Allow List security filter will automatically white list the allowed URLs to be accessed.

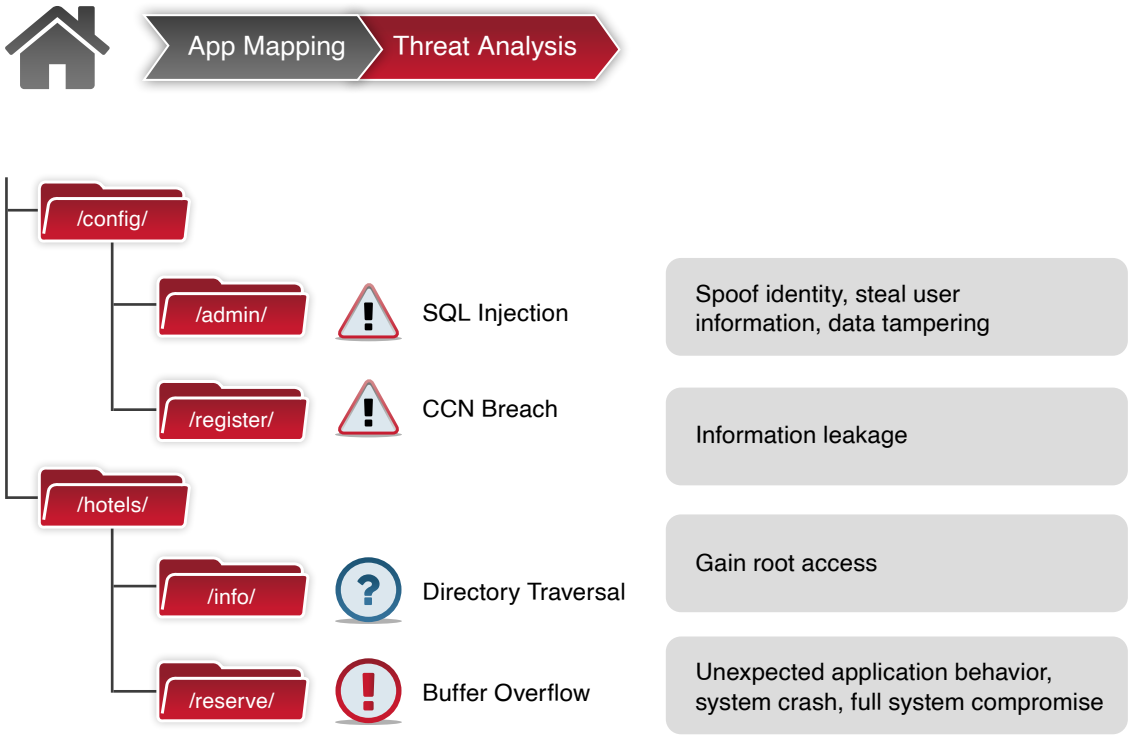
At the HTTP parsing module, various settings can be automatically optimized and modified by the systems. Examples for such automatic modification include message size settings for the request, and HTTP parsing properties exceptions, such as allowing High ASCII chars in the HTTP parameter value. Such HTTP RFC violation exceptions will be defined automatically either on specific URLs, or globally if required across many resources in the application.

Four Steps of Auto-Policy Generation

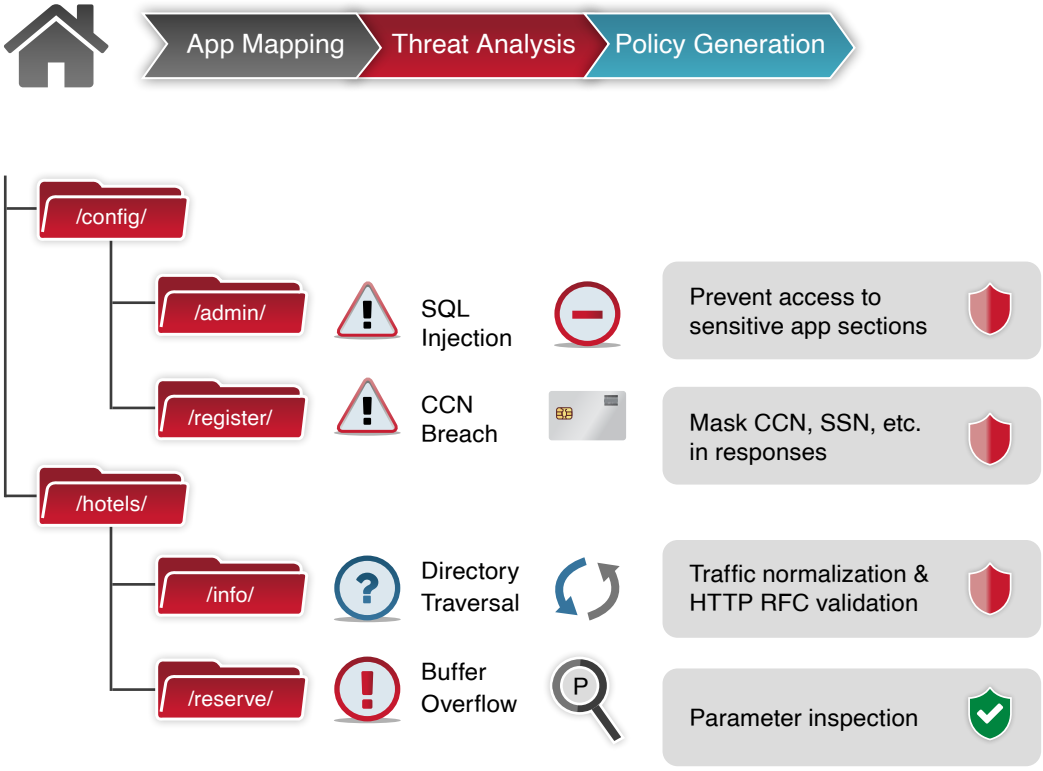
Step #1: Application mapping



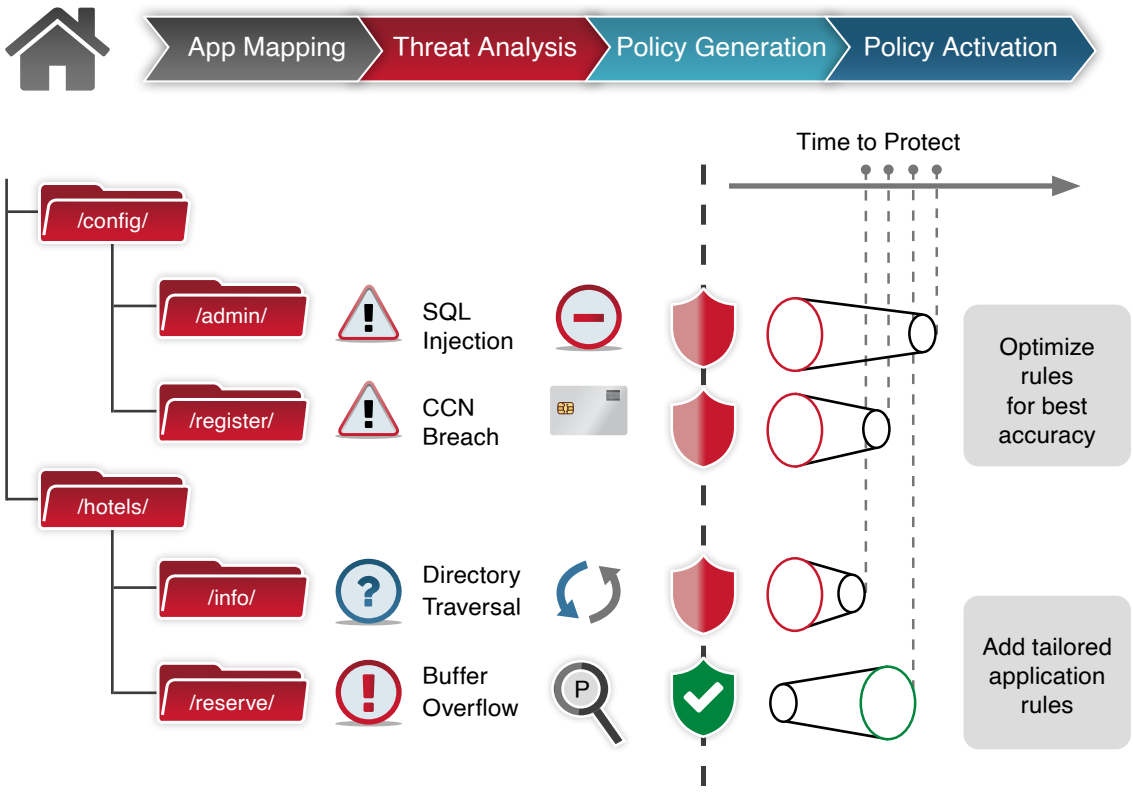
Step #2: Threat analysis – covering over 150 attack vectors



Step #3: Policy generation with auto-optimization for out-of-the-box rules to minimize false positives



Step #4: Policy activation



The Human Factor Behind the Automation

In Radware's Cloud WAF Service, once a policy is automatically generated, Radware's security experts review it to validate the quality of the generated policy in terms of validity of the policy, integrity, false positive risks, and false negative risks. This service is also available to Radware's WAF customers who choose to add the ERT Premium managed service.

Radware's security and cloud experts have extensive real-world experience providing protection from advanced cyberattacks with deep knowledge of Radware's WAF technology.

How Auto Policy Impacts the Quality of Protection

By eliminating the need for security policies to be manually set, Radware's auto policy provides superior protection while reducing human errors and operational costs/overhead.

The auto-policy generation system can learn and optimize different levels of protection, allow enabling ALL RULES, and activate various security filters. With this capability, the rules and filters are optimized and updated automatically, thereby removing the risk of generating false positives.

If we take a simple example of the Always True Expression type of SQL Injection such as " OR 1 = 1," we can easily understand that rules which are aimed to block such inputs will have a high tendency to generate false positives. If there is no automatic mechanism to create such policy exceptions, it will not be reasonable to define such rules which may block legitimate traffic. Most cloud WAF vendors do not define such risky rules.

Radware's Auto-Policy Generation allows enabling of all rules while automatically creating exceptions for these rules in areas where these rules generate false positives, while properly securing the rest of the application. For example, all HTTP RFC rules are enabled, while all injection rules are applied and being optimized automatically. This alone offers superior protection even if a positive security model isn't applied.

Shortest Time to Security

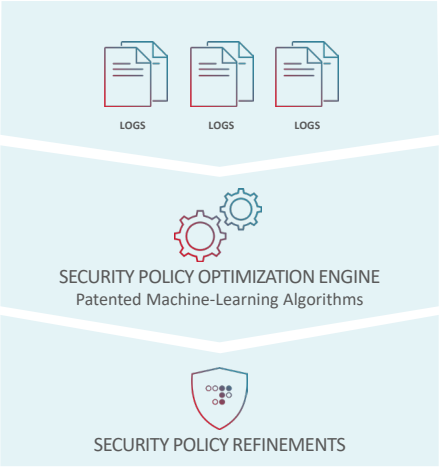
Radware's unique Auto-Policy Generation includes a set of machine-learning algorithms that analyze the protected application, generate granular protection rules and apply a security policy in blocking mode that offers the following benefits:

- **Shortest time to tailor-made protection**
- **Best security coverage by performing auto threat analysis, with no admin intervention** – covering over 150 attack vectors
- **Lowest false-positives** – achieved through auto-optimization of out-of-the-box rules, resulting in close to zero false positives
- **Automatic detection of web application changes assuring security throughout the application's development lifecycle** – post deployment peace of mind

Automated Continuous Security Policy Optimization

As applications continue to develop on a weekly and sometimes even on a daily basis, the threats also keep evolving. Therefore, it is important to constantly optimize WAF security polices to keep the security level as high as possible and reduce the number of false positives so that the legitimate traffic continues to flow uninterrupted.

A major challenge in application protection is to keep up with the rapid pace in which applications develop and the bombardment of new threats, that emerge every day, while achieving accurate security policies with minimum false positives. This requires hands-on management of security policies from beginning to end – going over logs with thousands of entries, and manually fine-tuning security rules. It is a tedious task that introduces lots of overhead and requires lots of time and effort, that do not always yield optimal results.



Radware's Automated Policy Optimization engine was developed to specifically address such challenges. The frictionless policy optimization engine is based on advanced machine-learning algorithms that automatically reviews large log files in pre-defined intervals, finds anomalies with high levels of accuracy, suggests policy refinements for Radware's ERT team to examine and prioritize, followed by review and approval by the customer for deployment. This is a continuous optimization process in which the machine runs automatically offline and policy refinements are implemented by the customer or Radware's ERT team at a click of a button. It is an error-proof mechanism with full control over the machine that provides:

- **More accurate, tighter protection** – Continuously improving and keeping itself relevant and updated to meet new threats
- **Fewer false positives** – No blocking of legitimate traffic
- **Higher operational efficiency** – Lower overheads and resource drainage

About Radware

Radware® (NASDAQ: RDWR), is a global leader of application delivery and cyber security solutions for virtual, cloud and software defined data centers. Its award-winning solutions portfolio delivers service level assurance for business- critical applications, while maximizing IT efficiency. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity and achieve maximum productivity while keeping costs down. For more information, please visit www.radware.com.

Radware encourages you to join our community and follow us on: Facebook, Google+, LinkedIn, Radware Blog, SlideShare, Twitter, YouTube, Radware Connect app for iPhone® and our security center DDoSWarriors.com that provides a comprehensive analysis on DDoS attack tools, trends and threats.

Certainty Support

Radware offers technical support for all of its products through the Certainty Support Program. Each level of the Certainty Support Program consists of four elements: phone support, software updates, hardware maintenance, and on-site support. Radware also has dedicated engineering staff that can assist customers on a professional services basis for advanced project deployments.

Learn More

To learn more about how Radware's integrated application delivery & security solutions can enable you to get the most of your business and IT investments, email us at info@radware.com or go to www.radware.com.

This document is provided for information purposes only. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law. Radware specifically disclaims any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The technologies, functionalities, services, or processes described herein are subject to change without notice.