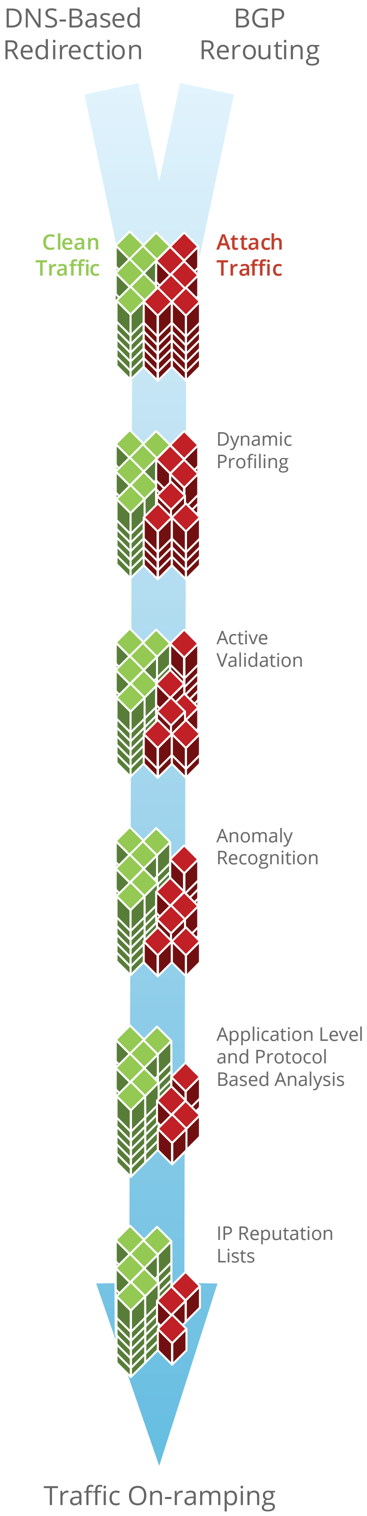
Cautela Labs **Web Application Firewall**

Protection and Monitoring application layer security for Web sites and Web Servers

Cautela Labs Web Application Firewall protects Web sites and Web applications from attackers leveraging protocol or application vulnerabilities to instigate data theft, denial of service, or defacement of an organization's Web site. Unlike traditional network firewalls or intrusion detection systems that simply pass HTTP, HTTPS, or FTP traffic for Web applications, the Cautela Labs Web Application Firewall proxies this traffic and inspects it for attacks to insulate Web servers from direct access by hackers.

Key Advantages

- OWASP Top 10 Vulnerability Protection
- Cross-site request forgery protection
- Automatic signature updates
- Strong authentication and authorization
- Information disclosure protection
- Robust dashboard
- Flexible policy settings
- Comprehensive audit log
- Cookie tampering protection
- Secure session management
- Anti-evasion measures
- HTTPS inspection
- Acceleration features
- Web site cloaking
- Custom rule chains
- Application profiling
- Geolocation-based policies
- Botnet filtering



Features & Capabilities

- **Open Web Application Security Project (OWASP) Top 10 Vulnerability Protection** addresses leading security risks based on prevalence and severity of attacks, as included in PCI DSS 6.6 and other industry standards.
- **DoS Protection** multiple protection policies for network and application layer denial of service threats. Sophisticated mechanism helps identify and block automated attacks.
- **Domain Name System Security Extensions (DNSSEC)** extension checks for all domains providing to DNS clients (resolvers) origin authentication of DNS data, authenticated denial of existence, and data integrity.
- **Antivirus** scan file uploads using Antivirus engine with regular signature updates.
- **High Availability and Multi-site configuration** provides synchronization and allows for a network-level failover in the event of unexpected outage events.
- **Protection against common attacks** is delivered in addition to protection against injection and cross-site scripting (XSS) attacks, SQL injection, OS command injection, Cookie or Forms tampering.
- **Automatic signature updates** and adaptive application profiling protect against known as well as emerging threats.
- **Web site cloaking** prevents hackers from guessing the web server implementation and exploiting any potential vulnerabilities.

Cautela Labs **Web Application Firewall**

- **Custom rule chains** allows the administrator to create custom rules/signatures in addition to the rules developed by Cautela Labs and Third Party Collaboration. It also allows the administrator to employ both positive and negative security models.

- **Application profiling** automatically suggests custom rules by intelligently learning from multiple offloaded web applications while also providing the ability to manage the generated custom rules on a per-portal basis.

- **Botnet filtering** leverages a dynamically updated database to identity and block rogue activity from compromised endpoints.

- **Flexible policy settings** enable administrators to apply signature settings based on threat severity as well as set exclusion list per signature.

- **Comprehensive audit log** makes logging and reporting available for auditing, compliance and reporting purposes.

- **Cookie tampering protection** minimizes the chances of a breach by modifying the cookies.

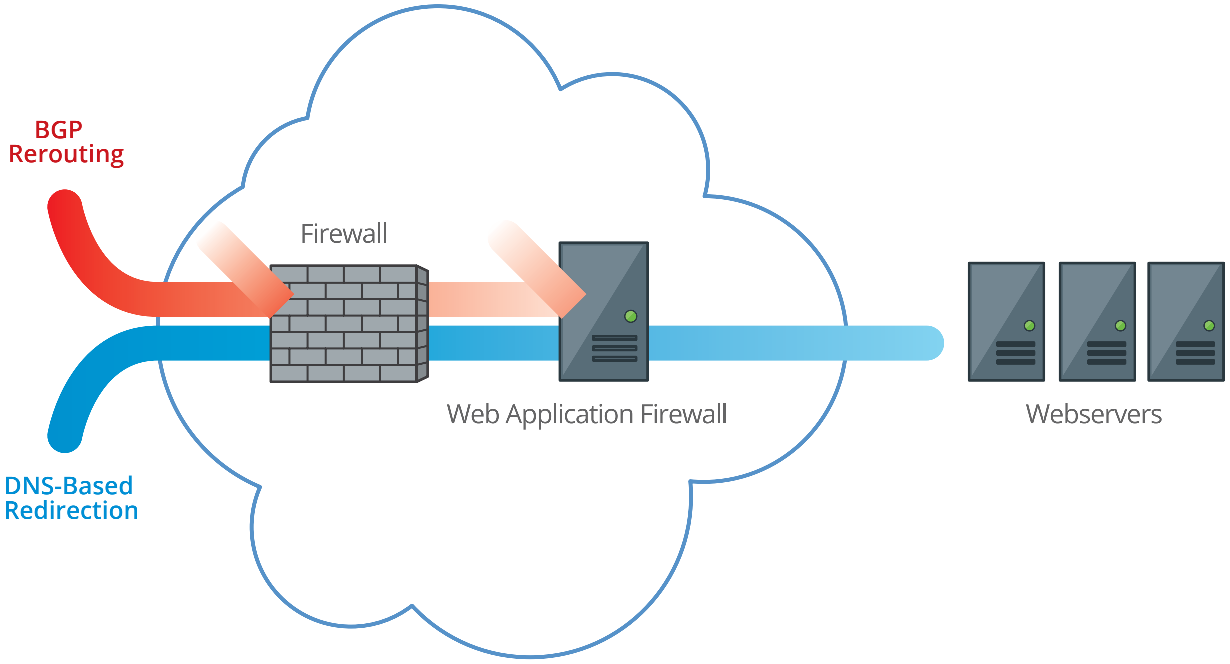
- **Session management** allows administrators to set global timeouts based on user inactivity.

- **Anti-evasion measures** normalize requests (e.g., standardizing encoded or suspect character sets or path names) prior to analysis.

- **HTTPS inspection** can block attacks embedded into SSL-encrypted packets.

- **Geo IP Analytics** analyze web usage from multiple vectors, map requests to their geographic location and easily block access from unwanted countries.

- **Additional Protection:** SMURF Attacks, Layer 3/4 attacks, DNS amplification attacks, ACK attacks, Layer 7 attacks.


BGP
Rerouting
Firewall
Web Application Firewall
Webservers
DNS-Based
Redirection