SOLUTION BRIEF

THUNDER WEB APPLICATION FIREWALL

STOP WEB ATTACKS TO PREVENT COSTLY DATA BREACHES

MOBILE USERS REQUIRE SECURE ALWAYS-ON NETWORK ACCESS

Web applications have become the number one battlefield in today's cyber war, pitting cybercriminals, hacktivists and state-sponsored attackers against enterprises and government agencies. Applications have catapulted to the frontlines of this war because they often represent the weak link in organizations' defenses. In fact, 96 percent of applications have vulnerabilities,[1] causing attackers to continually probe websites looking for weaknesses they can exploit.

To protect web applications, organizations need a solution that can mitigate attacks without blocking legitimate users and without slowing down application performance. They need a solution that is easy to configure and that supports detailed logging and graphical reporting.

The A10 Networks Thunder® ADC line of Application Deliver Controllers and Thunder Convergent Firewalls (CFW) each integrate a powerful and accurate Web Application Firewall (WAF) that stops web application attacks, probes and reconnaissance. Combining multiple layers of defense, Thunder WAF keeps out cybercriminals and hacktivists and prevents sensitive data leaks and mitigates the OWASP Top Ten list of security risks to keep applications safe.

Thunder WAF provides:

- Streamlined management with intuitive WAF templates
- White list and black list security models
- High performance and low latency powered by A10 Networks Advanced Core Operating System (ACOS®)
- Programmatic control over application traffic with A10 Networks aFleX® Deep Packet Inspection (DPI) Scripting Technology
- High-speed, CEF-compliant logging and graphical reporting
- PCI 6.6 compliance

[1] Cenzic Application Security Trends Report, 2014

CHALLENGE

Websites are under siege. Malicious users and bots continuously scan, probe and attack websites in order to detect and exploit vulnerabilities.

SOLUTION

A10 Thunder ADC and CFW solutions shield websites from attack with their high-performance, full-featured Web Application Firewall module.

BENEFITS

- Stop dangerous attacks like SQL injection, cross-site scripting and OWASP Top Ten risks
- Satisfy PCI compliance requirement 6.6
- Reduce operations costs with easy-to-configure templates and streamlined management
- Scale to protect high-traffic websites with A10 Networks Advanced Core Operating System (ACOS)
- Integrate attack protection, authentication and application delivery on a single platform

ESCALATING APPLICATION THREATS

Attackers bombard websites around the clock with attacks such as SQL injection, cross-site scripting (XSS) and cross-site request forgery (CSRF). Without dedicated protection against attack, hackers can exploit website vulnerabilities and steal data, resulting in costly breaches and brand damage.

Recent attacks on packaged applications have revealed a gaping hole in the age-old strategy to lock down applications by writing secure code. Because packaged applications are developed by third parties and not internally, organizations can't rely on secure coding processes to protect these applications. With 35% of all breaches caused by web attacks in 2013[2] organizations need a proactive defense to block web attacks.

Many organizations operate under a false sense of security, believing that their network firewalls and intrusion prevention systems can prevent application-layer threats. Unfortunately, these all-purpose security products do not provide the granularity or the specialized defenses to stop advanced web attacks.

THUNDER WAF SHIELDS YOUR WEB APPLICATIONS FROM ATTACK

To protect web applications, organizations need to deploy a Web Application Firewall that can mitigate a multitude of threat vectors and still deliver unmatched application performance. A10 Thunder ADC does just that: it leverages a shared memory architecture and 64-bit scalability to provide ironclad protection at high speed.

Thunder ADC and CFW include a full featured WAF that blocks web attacks before they can reach vulnerable applications. Deployed as a reverse proxy in front of web servers, Thunder WAF inspects web requests and responses and can block, sanitize or alert on web attacks. Thunder WAF uses multiple layers of defense to mitigate a wide range of web attacks and satisfy PCI 6.6 compliance.

With the Thunder ADC and CFW solutions, organizations can:

- **Prevent costly data breaches** – Provide robust protection against application threats, including the OWASP Top Ten[3] enabling organizations to avoid data theft and defacement. Incorporating white list and black list security as well as automated application learning, Thunder WAF can accurately pinpoint attacks. With the ability to sanitize input, Thunder WAF can render attacks harmless without disrupting users' application access.
- **Achieve PCI 6.6 compliance** – The Payment Card Industry Data Security Standard (PCI DSS) sets forth guidelines for merchants, processors and other entities to protect cardholder data. Thunder WAF enables organizations to satisfy PCI requirement 6.6.
- **Protect their data and their brand by preventing data leaks** – Thunder WAF can inspect outbound traffic for sensitive data like credit card and social security numbers. With easy-to-define Perl Compatible Regular Expressions (PCRE) masks, organizations can obfuscate custom strings, such as obscene words, from appearing in website forums.
- **Mitigate application vulnerabilities** – With out-of-the-box protection against web attacks like SQL injection and cross-site scripting, Thunder WAF can prevent hackers from exploiting website vulnerabilities. Customers can define custom aFleX scripting policies to "virtually patch" any remaining vulnerabilities, ensuring that applications are safe from abuse.
- **Protect sessions and cookies** – By optionally encrypting cookies, Thunder WAF can protect applications from threats such as cookie poisoning, cookie injection and session replay. Administrators can define which cookies to encrypt, allowing administrators to limit protection to sensitive, read-only cookies like session cookies.
- **Stop automated attacks** – Detect bots and automated clients by recognizing known bot agents. In addition, through request rate limiting and aFleX policies, block users who generate too many requests or do not behave like standard web clients. Block automated attacks originating from a specific region using IP geolocation.
- **Ensure that attackers cannot evade web defenses** – Thunder ADC and CFW normalizes each web request before inspecting it, ensuring that attackers cannot bypass the Web Application Firewall through obfuscation. Prevents buffer overflow attacks by setting accepted maximum

[2] Verizon 2014 Data Breach Investigation Report

[3] The Open Web Application Security Project (OWASP) Top Ten represents the ten most critical web application security flaws as de-termined by a broad consensus of security experts.

thresholds for aspects of HTTP requests, and blocking requests that exceed the configured limits.

- **Cloak server information to prevent website reconnaissance** – Modify HTTP response headers to "cloak" server information such as operating system or web server data. Since many types of attacks are specific to individual servers, operating systems and frameworks, server cloaking makes it much more difficult for hackers to exploit application vulnerabilities.
- **Prevent search engines from indexing sensitive data** – Block requests to password protected or private sections of a protected website originating from search engine IP addresses or user agents. Administrators can define policies to block access to specific web pages or to block specific user agents from the appliance web user interface.

With granular aFleX policies, administrators can construct advanced correlation policies that control access based on patterns in web server responses, source IP address, user agent and more.

- **Shield web applications from damaging DDoS attacks** – Stopping both network and application-layer Distributed Denial of Service (DDoS) attacks, Thunder appliances ensure uninterrupted application access. Select Thunder models include hardware-based Flexible Traffic Accelerator (FTA) technology to detect and block common DDoS attacks at exceptionally high speed.
- **Streamline management** – With intuitive WAF templates and automated learning policies, customers can easily configure and deploy the Thunder Web Application Firewall.

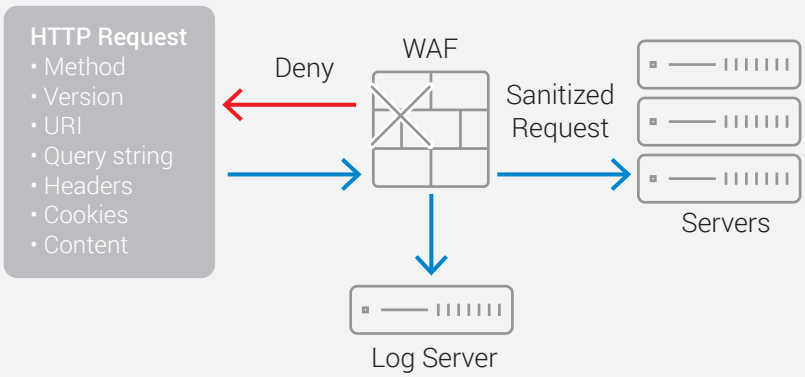

Figure 1: Thunder ADC and CFW, with their integrated WAF, can block attacks, sanitize requests of malicious content and log activity.

WEB APPLICATION FIREWALL FEATURES

WHITE LIST AND BLACK LIST SECURITY WITH AUTOMATED LEARNING

To stop web attacks, a WAF must recognize known good behavior as well as known attacks. The Thunder WAF automatically learns the structure of protected applications to detect unusual requests and attacks. By supporting multiple concurrent WAF templates, Thunder ADC and CFW appliances can learn new URLs and protect traffic at the same time.

Attack definition lists for SQL injection, cross-site scripting and more detect known attacks. Administrators can easily view and edit both black list and white list definitions from the web user interface or the CLI.

INTEGRATION WITH AFLEX SCRIPTING POLICIES

aFleX, an advanced scripting language for A10 Thunder appliances, provide the flexibility and power that administrators need to fully control their application traffic. aFleX is built on Tool Command Language (Tcl), an easy-to-learn scripting language, and it empowers customers to perform any number of actions, such as blocking traffic, redirecting traffic or modifying content.

Since WAF rules can integrate with aFleX policies, administrators can granularly control WAF behavior. For example, administrators can create exceptions to ignore specific violations or apply more stringent policy enforcement based on source IP address or destination URL.

aFleX also enables WAF administrators to apply custom rules to "virtually patch" vulnerable web applications until the underlying application is patched. Because of the flexibility of the aFleX scripting language, customers can solve almost any type of web application security challenge with a few simple lines of script.

GEOLOCATION TO MONITOR OR BLOCK ACCESS BY COUNTRY

With the rise of hacktivism and cyber espionage, organizations increasingly need to restrict access based on location. A10's geolocation policies make it easy to apply geolocation controls. By importing third-party geolocation lists from customers' preferred geolocation services, A10 customers can alert on or block traffic originating from specific regions. Location-based controls enable A10 customers to stop DDoS attacks initiated from certain countries and to meet export compliance requirements.

XML AND JSON PROTECTION

XML and JavaScript Object Notation (JSON) power many of today's leading websites. Dynamic and interactive applications often use JSON to update web data in near real time. Thunder WAF can inspect JSON traffic for attacks like SQL injection or XSS and can limit JSON elements such as array length or structure depth. Thunder WAF can also parse and inspect XML files and enforce Web Services Description Language (WSDL) schemas to ensure that XML files are formatted correctly.

INTEGRATED LOAD BALANCING, AUTHENTICATION AND DDOS PROTECTION

Thunder ADC and CFW appliances helps organizations simplify and consolidate their network architectures by delivering a complete solution for application delivery and security. Thunder ADC and CFW solutions load balance web traffic, monitors server health with advanced health checks, and accelerates performance with caching, compression and TCP optimization. Application Access Management (AAM) provides authentication and authorization, while DDoS protection stops application and volumetric DDoS attacks – scaling to block over 200 million SYN packets per second on a single device.

COMPREHENSIVE AND SCALABLE MANAGEMENT

To streamline and automate management, Thunder appliances include an industry standard CLI, a web user interface and a RESTful API (A10 Networks aXAPI® REST-based API) which can integrate with third-party or custom management consoles. For larger deployments, A10 Networks aGalaxy® Centralized Management System ensures that routine tasks can be performed at scale across multiple Thunder appliances, regardless of physical location.

LOGGING AND REPORTING

Thunder appliances support high-speed syslog logging as well as email alerts and NetFlow and sFlow statistics for traffic analysis. Graphical reports document security trends for attack analysis and compliance, while a real-time dashboard displays system information, memory and CPU usage, and network status.

HARDWARE AND VIRTUAL APPLIANCES

Thunder ADC and CFW are a family of hardware and software appliances that support a wide variety of deployment needs. Our Thunder hardware appliances provide maximum reliability and performance, scaling from 5 to 220+ Gbps of throughput in a single appliance. To support virtualized and cloud computing environments, A10 offers vThunder® ADC and CFW lines of virtual appliances for an array of hypervisors, while A10 Networks Thunder hybrid virtual appliances (HVA)

combine the flexibility of a virtual appliance and the power of a performance optimized hardware appliance.

A10's Web Application Firewall, included with Thunder ADC and CFW without additional license fees, enables organizations to quickly and cost-effectively secure their web applications. Powered by ACOS and its high-speed shared memory architecture, Thunder ADC and CFW load balances and protects applications at scale, without requiring organizations to purchase separate web application firewalls or to upgrade existing load balancers.

WEB APPLICATION FIREWALL SPECIFICATIONS

WEB APPLICATION ATTACK MITIGATION

- SQL injection attack protection
- Cross-site scripting attack protection
- Cross-site request forgery (CSRF) attack protection
- Open redirect attack protection
- Bot defenses by detecting known bot agents and frequency of requests
- Buffer overflow mitigation
- Attack evasion techniques by normalizing traffic and enforcing protocol compliance

Supported Protocols

HTML, DHTML, XML, SOAP, JSON, AJAX

HTTP/1.0 and HTTP/1.1

APPLICATION DEFENSES

- HTTP protocol conformance
- White list security with automated learning
- Black list security
- Request normalization
- Cookie encryption, URI and form rewriting for session protection
- Client-side caching and SSL security enhancements
- Blocking by geolocation
- aFleX policies for customized rules and complete programmatic control

DATA LOSS PREVENTION

- Credit card and social security number masking
- Perl Compatible Regular Expressions (PCRE) pattern matching
- Response cloaking

AUTHENTICATION

- Basic
- Digest
- NT LAN Manager (NTLM)
- Client SSL certificate
- Security Assertion Markup Language (SAML)
- oken-based authentication

DDOS PROTECTION

- Volumetric DDoS attacks – SYN flood, ICMP flood, UPD flood, Ping of Death, Smurf attack, LAND attack, fragmented packets
- Application-layer DDoS attacks – HTTP flood, Slowloris, Slow POST, DNS flood, targeted attacks to exhaust backend database resources

PROTECT YOUR WEB APPLICATIONS WITH THUNDER WAF

With escalating threats like SQL injection, XSS and application-layer DDoS attacks, organizations need a solution that can safeguard their web applications.

Organizations can depend on Thunder's WAF to protect their applications and data and deliver a powerful defense against web attacks. Built on A10's Advanced Core Operating System (ACOS) platform, Thunder ADC and CFW platforms with WAF offer exceptional performance that enables customers to support future scalability and feature requirements.

With its integral role protecting applications using its integrated WAF, as well as its advanced DDoS protection, DNS firewall, SSL inspection and authentication features, Thunder ADC and CFW have become the security platform of the data center. Trusted by thousands of organizations around the world, these solutions ensure that applications are highly available, accelerated and secure.

ABOUT A10 NETWORKS

A10 Networks (NYSE: ATEN) is a Secure Application Services™ company, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, Calif., and serves customers globally with offices worldwide.

For more information, visit: a10networks.com
or tweet @a10Networks

LEARN MORE

ABOUT A10 NETWORKS

CONTACT US

a10networks.com/contact

Part Number: A10-SB-19128-EN-03 SEP 2017