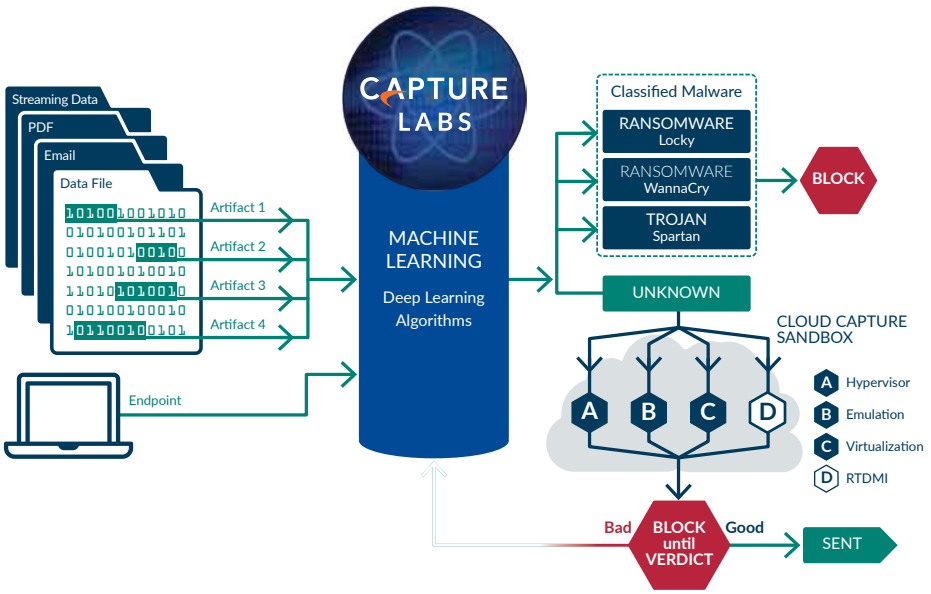
Web Application Firewall

SonicWall Web Application Firewall offers a comprehensive foundation for web application security, data leak prevention and performance, on prem or in the cloud

The SonicWall Web Application Firewall (WAF) Series enables a defense-in-depth strategy to protect your web applications running in a private, public or hybrid cloud environment. It offers a complete, out-of-box compliance solution for application-centric security that is easy to manage and deploy.

The SonicWall WAF is a full-featured web application firewall that arms organizations with advanced web security tools and services to protect their data and web properties against modern, web-based threats. It applies deep packet inspection of Layer 7 web traffic against a regularly updated database of known signatures, denies access upon detecting web application vulnerabilities and redirects users to an explanatory error page. This helps keep compliance data unexposed and web properties safe, undisrupted and in peak operating performance. WAF learns, interrogates and baselines regular web application usage behaviors and identifies anomalies that may be indicative of attempts to compromise the application, steal data and/or cause service disruption.

WAF employs a combination of signature-based and application profiling deep-packet inspection. Its high performance real-time intrusion scanning engine uses event-driven architecture to dynamically defend against evolving threats. These include those outlined by the Open Web Application Security Project (OWASP), as well as more advanced web application threats like Denial of Service (DoS) attacks and context-aware exploits. Moreover, WAF also prevents data loss with data masking and page-blocking techniques for specified patterns of sensitive data like Payment



Benefits:

Web Application Threat Management

- Shrink attack surface with full management and control of web application traffic
- Interrogate the behavior and logic of web communication beyond protocol activities
- Detect and alert on anomalies in web application behavior

Web Application Protection

- Protect against known and zero-day vulnerabilities with Capture ATP, virtual patching and custom rules
- Defend against latest vulnerabilities and threats outlined by OWASP Top Ten
- Preserve web servers' integrity and performance against application DoS/DDoS attacks

Data Leak Prevention (DLP)

- Prevent data theft via data masking and page-blocking techniques
- Bar attackers from gaining access to users' accounts and all accounts on web servers with precise access security controls

Accelerate Application Delivery

- Enable caching, compression and other HTTP/TCP optimizations to accelerate application delivery
- Reduce workload and boost performance by offloading SSL transactions
- Perform Layer-7 load balancing to distribute the load across clustered web servers

Card Information (PCI) and government issued identification.

For optimal protection against malicious downloads, malware injections or advanced threats, WAF leverages SonicWall Capture Labs threat research. It also adds SonicWall Capture Advanced Threat Protection (ATP) and Real-Time Deep Memory Inspection (RTDMI™) service options to its suite of web security services. Additionally, APIs are provided to give administrators the ability to monitor and orchestrate WAF operations programmatically for improved web security automation and efficiency.

Cross-vector threat intelligence

Capture Labs performs threat hunting and intelligence sharing across the entire SonicWall security ecosystem including WAF. The research team vets cross-vector threat information from a variety of sources, including a million globally placed security sensors while continuously developing and patching WAF with dynamic threat signatures for up-to-date web application protection.

Multi-engine advanced threat analysis

SonicWall Capture ATP Service extends web application protection to detect and prevent zero-day attacks. Suspicious file downloads or injections are sent to the SonicWall Capture ATP service in the cloud for analysis using deep learning algorithms. It has the option to hold them at the gateway until a verdict is rendered.

Unique only to SonicWall, this multi-engine sandbox platform applies a combination of third-party and proprietary static and dynamic processing tools for threat prevention. These include a pool of over 60 reputable virus scanners, RTDMI, virtualized sandboxing, full system emulation and hypervisor-level analysis technologies.

Simultaneously, each inspection technique executes suspicious code and analyzes behavior and provides comprehensive visibility to malicious activity. At the same time, it resists evasion tactics for optimized zero-day threat discovery and defense.

Let's Encrypt integration

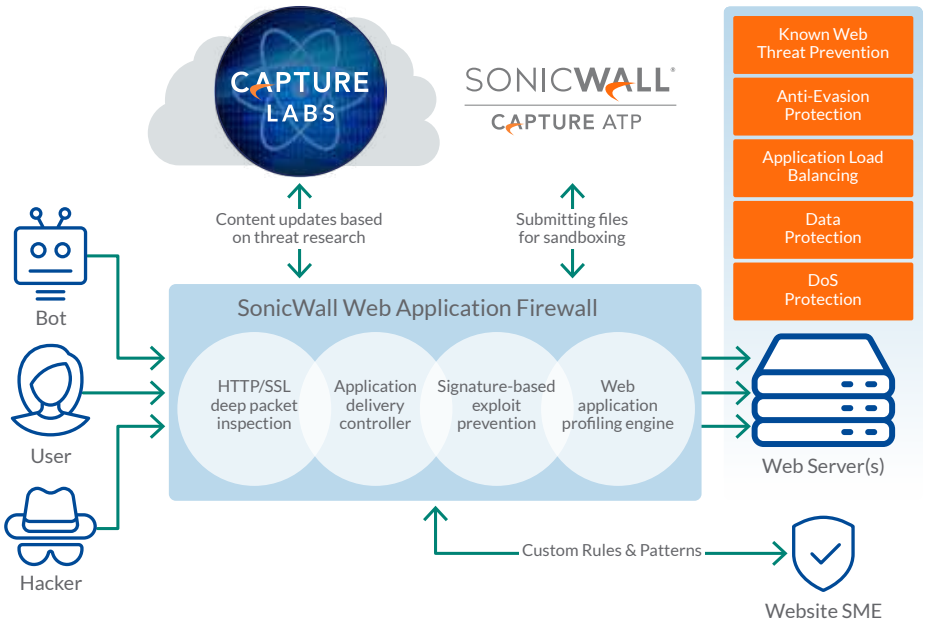
To help organizations deliver greater security to website visitors and elevate their SEO placement, WAF integrates with the Let's Encrypt service. This complimentary Certificate Authority (CA) service includes issuing, monitoring, renewing and decommissioning certificates, for easy SSL/TLS certificate life-cycle management. Completely managed by the SonicWall WAF, customers can easily implement HTTPS for their websites using this service.

Economy of Scale

WAF provides economy of scale benefits of virtualization and can be deployed as a virtual appliance in private clouds based on VMWare or Microsoft Hyper-V; or in AWS or Microsoft Azure public cloud environments. This gives organizations all the security advantages of a physical WAF with the operational and economic benefits of virtualization, including system scalability and agility, speed of system provisioning, simple management and cost reduction.

Acceleration features include load balancing, content caching, compression and connection multiplexing improve performance of protected websites and significantly reduce transactional costs. A robust dashboard provides an easy-to-use, web-based management interface. This features status page overview of all monitoring and blocking activities, such as signature database status information and threats detected and prevented since boot-up.

The WAF Series is available in four website models that represent their licensed inspection capacities to accommodate various monthly traffic volume with unlimited domain. The



subscribed Licensed Capacity activates WAF's complete suite of security services up to the prescribed monthly capacity. Services include Capture ATP with RTDMI™ technology to inspect web traffic and web transactions. It then resets each month. Licensed Capacity options are stackable to address growing capacity needs.

Deployment options

SonicWall WAF can be deployed on a wide variety of virtualized and cloud platforms for various private/public cloud security use cases. The WAF Series is available for deployment on the following platforms:

1. Private Cloud:
   - VMware ESXi
   - Microsoft Hyper-V
2. Public Cloud:
   - Amazon Web Services (AWS)
   - Microsoft Azure

WEBSITE MODEL	LICENSED CAPACITY
PRO	10 GB per Month
SMALL	50 GB per Month
MEDIUM	200 GB per Month
LARGE	500 GB per Month

Summary of WAF Features

Web Application Security

- OWASP Top 10 Protection
- CSRF Protection
- Cookie Tampering Protection
- Website Fingerprint Detection
- Sensitive Data Protection - Masking and Blocking
- Rate Limiting and DoS Protection
- Anti-evasive inspection
- Automatic Signature updates
- Web Application Profiling & Auto-Rule Generation
- Access Policies (using Geo, IP, URL or User)
- Custom Rules & Rule-chaining
- Custom Error response
- Secure Session Logout
- HTTP Strict Transport Security (HSTS) Support
- Let's Encrypt service
- Authentication with MFA support

Capture advanced threat protection

- Real-Time Deep Memory Inspection
- Cloud-based multi-engine analysis
- Virtualized sandboxing
- Hypervisor level analysis
- Full system emulation
- Broad file type examination
- Automated and manual submission
- Real-time threat intelligence updates
- Block until verdict

Botnet Protection

- Geo-IP- and Threat Intel-based protection filtering
- Blacklisting and Whitelisting
- Blocking and Captcha-based Remediation Support

Secure Web Application Delivery

- Secure Web App. Offloading
- SSL Inspection & PFS
- Session Logout Timer
- Layer-7 Load Balancing
- Web App. Health Monitoring
- Web App. Acceleration -content caching, compression and TCP optimization

Administration

- Customizable Web Portal with CLI Support
- Admin Authentication via AD/LDAP, RADIUS and Certificate
- Automatic Software Updates
- API Support

Monitoring & Reporting

- SNMP Support
- Event / Audit Logging & Syslog
- Email alerts
- System monitoring & Diagnostics
- Threats Dashboard
- Health Dashboard
- PDF Report Exports

Platforms & Licensing

- VMWare & MS Hyper-V and AWS & MS Azure (BYOL)
- Subscription License based on capacity

Partner Enabled Services

Need help to plan, deploy or optimize your SonicWall solution? SonicWall Advanced Services Partners are trained to provide you with world class professional services. Learn more at www.sonicwall.com/PES.

Features

Web Application Security and Bot Protection	
OWASP Top 10 Protection	Protection of web applications from top 10 known attacks from the Open Web Application Security Protection (OWASP) including SQL Injection, XSS/CSRF, Web Fingerprinting, etc.
Sensitive Data Protection	Prevent sensitive data loss prevention with the ability to block pages presenting sensitive data and masking Personally Identifiable Information (PII) like credit card numbers and social security numbers
Session Management Controls	Provide strong session management and authentication capabilities to enhance the authorization requirements such One Time Password, Two-factor Authentication, Single Sign-On, and client certificate authentication.
Web-Form Input Validation	Inspect and validate client requests for possible malicious code to protect the backend servers from transactions that could allow hackers to bypass security defenses.
Session Hijacking Monitoring	Detect eavesdropping, intrusion and even theft of a web sessions to help prevent malicious actions taken by the attacker.
Secure Session Logout	Provide the ability to safely and securely logout of a Web App that has been authenticated by a WAF.
Perfect Forward Secrecy (PFS) prevention	Protect past sessions against future compromises of secret keys or passwords.
Deny Cross-Site Request Forgery (CSRF) attacks	Recognize and prohibit malicious websites from sending illegitimate requests to a web application that a user is already authenticated against from a different website.
Block code injection or remote code-inclusion attacks	Recognize and disrupt attacks that exploit a web application's interface to the underlying operating system and results in the unwanted execution of arbitrary code or harmful commands, such as the download a malicious payload.
Cookie Tampering Protection and Encryption	Protect against cookie theft, poisoning, inaccuracies, and Cross-Site Cooking via encryption and exclusion.
Rate Limiting for Custom Rules	Track the rate at which a custom rule, or rule chain, is being matched to block dictionary attacks or brute force attacks.
Web server Fingerprint Protection	Defend against web server fingerprinting attacks that identify web application software, its version and the platform that help hackers exploit vulnerabilities reported in the software.
Web services/API protection	Prevent exposure of the valuable information contain within web services and APIs.
API Support	Give administrators the ability to monitor and orchestrate WAF operations programmatically without using the management web interface.
CMS platform protection:	Use custom rules with virtual patching to neutralize new vulnerabilities found in popular CMS tools, such as WordPress, Joomla, and Documentum.
Denial of Service Protection	Rate-limiting and bandwidth throttling of traffic to web applications for Denial of Service (DoS) protection of web applications.
Automatic Signature Updates	Periodic automated updates of signatures based on research from Capture Labs of new and emerging web application threats
Web Application Profiling	Unique profiling engine that monitors known good activity against a web application to establish a baseline and automatically generates WAF rules for that web application. Supports the use of trusted IP addresses for baselining.
Custom Rules & Error Response	Ability to create custom rules based on application-specific logic along with creation of rule-chains for serialized logic. Customizable block pages and error messages when rules are matched.
Botnet Filtering & Remediation	Botnet filtering based on geography, explicit IP addresses/ranges and leveraging built-in threat intelligence integration. Support for remediation via captchas for each type of botnet filter. Also supports creation of blacklists and whitelists.
HTTP Strict Transport Security (HSTS) Support	Policy mechanism to force browsers and apps connections to use HTTPS encryption for secured web communication and data exchange. This helps protect against protocol downgrade attacks and cookie hijacking.
Let's Encrypt service	Integrated with the Let's Encrypt service for easy SSL/TLS certificate life-cycle management. This includes issuing, monitoring renewing and decommissioning certificates.
Authentication with MFA support	Authentication of users to websites and URLs with existing authentication services offered by the website or by injecting an explicit authentication mechanism of its own. These mechanisms can also be stacked (e.g. 2FA, OTP) for multi-factor authentication to sensitive web pages.

Capture Advanced Threat Protection	
Multi-engine sandboxing	The multi-engine sandbox platform, which includes virtualized sandboxing, full system emulation, and hypervisor level analysis technology, executes suspicious code and analyzes behavior, providing comprehensive visibility to malicious activity.
Real-Time Deep Memory Inspection (RTDMI)	This patent-pending cloud-based technology detects and blocks malware that does not exhibit any malicious behavior and hides its weaponry via encryption. By forcing malware to reveal its weaponry into memory, the RTDMI engine proactively detects and blocks mass-market, zero-day threats and unknown malware.
Block until verdict	To prevent potentially malicious files from entering the network, files sent to the cloud for analysis can be held at the gateway until a verdict is determined.
Broad file type and size analysis	Supports analysis of a broad range of file types, including executable programs (PE), DLL, PDFs, MS Office documents, archives, JAR, and APK plus multiple operating systems including Windows, Android, Mac OS X and multi-browser environments.
Rapid deployment of signatures	When a file is identified as malicious, a signature is immediately deployed to firewalls with SonicWall Capture ATP subscriptions and Gateway Anti-Virus and IPS signature databases and the URL, IP and domain reputation databases within 48 hours.

Secure Application Delivery	
Secure Web Application Offloading	Deployed as a Reverse Proxy to offload application front-ending. Also includes the ability to auto-logout user sessions after specific inactivity periods.
SSL Inspection	Built-in support for both HTTP and SSL/TLS traffic, with the ability to receive SSL/TLS traffic and forward as HTTP to web applications. Ability to import and store SSL certificates with support to broker Certificate Signing Requests (CSRs) and CRL validation.
Layer-7 Load Balancing	Easy to use Load-balancing features with session persistence, customizable logic and failover support that also delivers web application health monitoring.
Web Application Acceleration	Leverage a combination of content caching, content compression and network bandwidth optimization to deliver accelerated website experiences

Management	
Web Portal & Command Line Interface	Familiar web portal for GUI-based administration with customizable look and feel including logos (for Service Providers). Additional support also for CLI-based administration
Administrator Authentication	Support for multiple forms of administrator authentication including MS Active Directory, LDAP, RADIUS and Certificate-based authentication. Includes Password strength enforcement and role-based authorization.
Software Updates	Automated software updates from SonicWall Cloud that are automatically downloaded and applied for all licensed WAFs

Monitoring & Reporting	
Logging & Alerting	Granular logging for security, system and audit events with the flexibility to control log levels and configure log transfer via Syslog to external systems like SIEM platforms. Severity-based email-based alerting of events
System Monitoring & SNMP Support	Extensive system diagnostics using debug modes and with auto-generation of Technical Support reports (TSRs). Support for 3rd party monitoring using SNMP with easily downloadable MIBs
Dashboards & Reports	Intuitive dashboards for Top Web Security & Botnet Threats, Latest Alerts and for Web Application Health and Performance. Comparative dashboards against global threat status with Capture Labs support. Downloadable reports in PDF format

Platforms & Licenses	
Platforms	Delivered as a virtual appliance that can be deployed on private cloud hypervisors VMWare and MS Hyper-V, as well as public clouds AWS and MS Azure. For AWS and Azure, the Bring-Your-Own-License models is supported
License Model	Procured as a Subscription License with a termed entitlement of use and includes 24x7 Support Services. Available in different “models” based on capacity and in single-year and multi-year SKUs.

Ordering Information

PRODUCT	SKU
SonicWall WAF for 1 PRO Website 10 GB Monthly With 24x7 Support 1-year	02-SSC-0851
SonicWall WAF for 1 PRO Website 10 GB Monthly With 24x7 Support 3-year	02-SSC-0852
SonicWall WAF for 1 Small Website 50 GB Monthly With 24x7 Support 1-year	02-SSC-0854
SonicWall WAF for 1 Small Website 50 GB Monthly With 24x7 Support 3-year	02-SSC-0853
SonicWall WAF for 1 Medium Website 200 GB Monthly With 24x7 Support 1-year	02-SSC-0856
SonicWall WAF for 1 Medium Website 200 GB Monthly With 24x7 Support 3-year	02-SSC-0855
SonicWall WAF for 1 Large Website 500 GB Monthly With 24x7 Support 1-year	02-SSC-0858
SonicWall WAF for 1 Large Website 500 GB Monthly With 24x7 Support 3-year	02-SSC-0857

About Us

SonicWall has been fighting the cybercriminal industry for over 27 years, defending small, medium-sized businesses and enterprises worldwide. Our combination of products and partners has enabled an automated real-time breach detection and prevention solution tuned to the specific needs of the more than 500,000 organizations in over 215 countries and territories, so you can do more business with less fear. For more information, visit **www.sonicwall.com** or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com