SONICWALL

Web Application Firewall

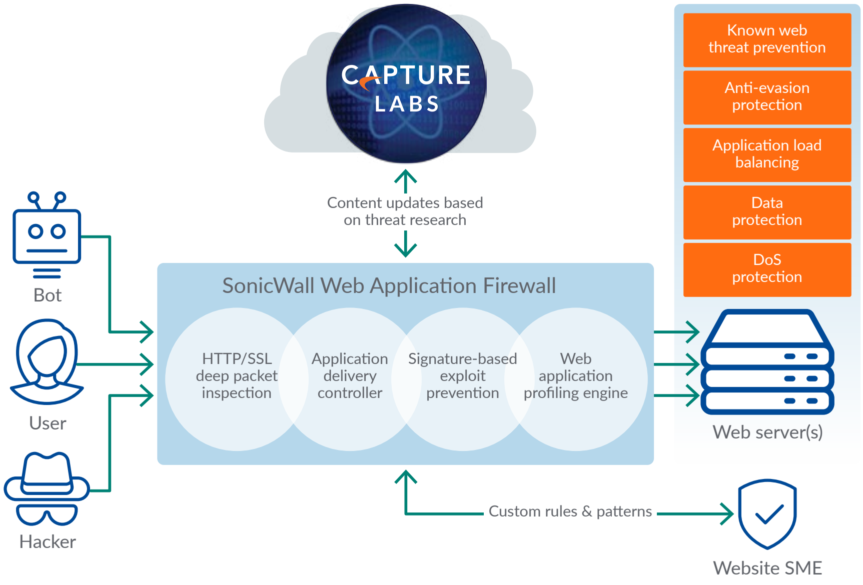
SonicWall Web Application Firewall offers a comprehensive foundation for web application security, data leak prevention and performance, on prem or in the cloud

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

The SonicWall WAF Series is 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 threats and redirects users to an explanatory error page. In addition, the SonicWall WAF also baselines regular web application usage / behavior and identifies anomalies that may be indicative of attempts to compromise the application, steal data and/or cause a denial-of-service.

WAF employs a combination of signature-based and application profiling deep-packet inspection, and high performance real-time intrusion scanning engine using event-driven architecture to dynamically defend against evolving threats as 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, it 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 a denial-of-service.

WAF provides economy of scale benefits of virtualization and can be deployed as a


CAPTURE LABS
Content updates based on threat research
Known web threat prevention
Anti-evasion protection
Application load balancing
Data protection
DoS protection
Bot
User
Hacker
SonicWall Web Application Firewall
HTTP/SSL deep packet inspection
Application delivery controller
Signature-based exploit prevention
Web application profiling engine
Web server(s)
Custom rules & patterns
Website SME

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 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

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 featuring status page overview of all monitoring and blocking activities, such as signature database status information and threats detected and prevented since boot-up.

The Series is available in four models that represent their inspection capacities and can be deployed on a broad range of public/private cloud/virtualized deployment use cases.

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

MODEL	COMPUTE CAPACITY	RECOMMENDED AWS INSTANCE	RECOMMENDED MS AZURE INSTANCE
WAF 200	2 vCPU	C5.large	Standard_F2s_v2
WAF 400	4 vCPU	C5.xlarge	Standard_F4s_v2
WAF 800	8 vCPU	C5.2xlarge	Standard_F8s_v2
WAF 1600	16 vCPU	C5.4xlarge	Standard_F16s_v2

**Based on using server-grade compute processors like Intel Xeon E5-2600 series*

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

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
- Stacked Authentication (2FA, OTP, client-cert, etc.)
- Session Logout Timer
- Layer-7 Load Balancing
- Web App. Health Monitoring
- Web App. Acceleration -content caching, compression and TCP opt

Administration

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

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

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.
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.
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.

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.
Stacked Authentication	Support for applying stacked authentication in front of a protected web application for multi-factor authentication or enforced authentication for unsupported web applications
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 also available in single-year and multi-year SKUs.

System Specifications

	WAF 200	WAF 400	WAF 800	WAF 1600
Supported Platform	VMware ESXi v6.5 Microsoft Hyper-V Manager 6.2 / 6.3 Amazon AWS Microsoft Azure			
WAF Tier	Tier 1	Tier 2	Tier 3	Tier 4
SSL Transactions/sec	6,000	12,000	24,000	48,000
SSL Throughput	500 Mbps	1 Gbps	2 Gbps	4 Gbps
Recommended vCPUs*	2	4	8	16
Recommended Memory	4 GB	8 GB	16 GB	32 GB
Recommended Storage	8 GB	8 GB	8 GB	8 GB
Recommended AWS Instance	c5.large	c5.xlarge	c5.2xlarge	c5.4xlarge
Recommended Azure Instance	Standard_F2s_v2	Standard_F4s_v2	Standard_F8s_v2	Standard_F16s_v2

This is based on typical enterprise-grade server systems. For more information, please see the Deployment Guides.

Ordering Information

PRODUCT	SKU
SonicWall WAF 200 With 24x7 Support 1yr	01-SSC-4639
SonicWall WAF 200 With 24x7 Support 2yr	01-SSC-4638
SonicWall WAF 200 With 24x7 Support 3yr	01-SSC-4637
SonicWall WAF 400 With 24x7 Support 1yr	01-SSC-6299
SonicWall WAF 400 With 24x7 Support 2yr	01-SSC-4567
SonicWall WAF 400 With 24x7 Support 3yr	01-SSC-6314
SonicWall WAF 800 With 24x7 Support 1yr	01-SSC-4597
SonicWall WAF 800 With 24x7 Support 2yr	01-SSC-6379
SonicWall WAF 800 With 24x7 Support 3yr	01-SSC-6319
SonicWall WAF 1600 With 24x7 Support 1yr	01-SSC-4560
SonicWall WAF 1600 With 24x7 Support 2yr	01-SSC-4562
SonicWall WAF 1600 With 24x7 Support 3yr	01-SSC-4561

About Us

SonicWall has been fighting the cyber-criminal industry for over 25 years, defending small, medium size businesses and enterprises worldwide. Our combination of products and partners has enabled a real-time cyber defense solution tuned to the specific needs of the more than 500,000 businesses in over 150 countries, so you can do more business with less fear.

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