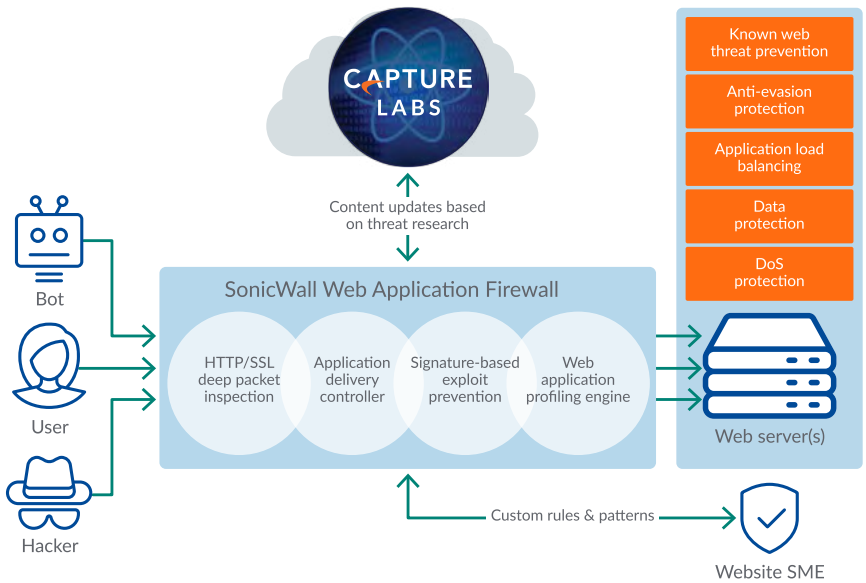
Web Application Firewall (WAF)

SonicWall Web Application Firewall to kompleksowa platforma bezpieczeństwa aplikacji webowych, ochrony przed wyciekiem danych oraz zwiększania wydajności, do uruchamiania lokalnie bądź w chmurze

Dzięki platformie Web Application Firewall (WAF) firmy SonicWall możliwe staje się stworzenie strategii zaawansowanej ochrony aplikacji webowych uruchamianych w środowiskach chmury prywatnej, publicznej bądź hybrydowej. WAF oferuje organizacjom kompletne i gotowe do działania rozwiązanie ułatwiające zachowanie zgodności z regulacjami oraz ochronę aplikacji, którą można łatwo wdrożyć i zarządzać.

Seria SonicWall WAF to w pełni funkcjonalny firewall aplikacyjny, który zapewnia organizacjom zaawansowane narzędzia ochrony webowej i usługi zabezpieczające dane oraz zasoby webowe przed nowymi zagrożeniami wykorzystującymi Internet. Ochrona opiera się na głębokiej inspekcji pakietów w warstwie 7 ruchu webowego (skorelowanej z regularnie aktualizowaną bazą znanych sygnatur), a także blokowaniu dostępu po wykryciu zagrożeń dla aplikacji webowej z przekierowywaniem użytkowników na specjalną stronę objaśniającą zdarzenie. Dodatkowo SonicWall WAF określa typowe wykorzystanie/zachowanie aplikacji webowych, identyfikując anomalie, które mogą wskazywać na próby obejścia zabezpieczeń aplikacji, kradzieży danych lub blokowania usług (atak denial-of-service).

WAF wykorzystuje kombinację sygnaturowej i aplikacyjnej głębokiej inspekcji pakietów oraz wydajnego mechanizmu wykrywania włamań w czasie rzeczywistym. Jego architektura umożliwia dynamiczną obronę przed szybko ewoluującymi zagrożeniami, zgodnie z OWASP (Open Web Application Security Project), oraz zabezpiecza przed zaawansowanymi atakami na aplikacje webowe, takimi jak Denial of Service (DoS) i exploity typu context-aware. Dodatkowo WAF uczy się i ustala typowe wykorzystanie aplikacji webowej, identyfikując anomalie mogące wskazywać na próby obejścia zabezpieczeń, kradzieży danych lub blokowania usług.



Funkcjonalności i korzyści:

Zarządzanie zagrożeniami dla aplikacji webowych

- Ogranicza pole ataku, dzięki pełnemu zarządzaniu i kontroli ruchu związanego z aplikacjami webowymi
- Koreluje zachowanie i logikę komunikacji webowej wykraczającą poza aktywność protokołów
- Wykrywa i zawiadamia o anomaliach w zachowaniu aplikacji webowych

Ochrona aplikacji webowych

- Chroni przed znanymi podatnościami oraz lukami typu zero-day dzięki funkcji wirtualnego łatania i regułom własnym
- Chroni przed ostatnio wykrytymi lukami i zagrożeniami opisywanymi przez OWASP Top Ten
- Zabezpiecza integralność i wydajność serwerów webowych, chroniąc przed atakami DoS/DDoS na aplikacje

Ochrona przed wyciekiem danych (DLP)

- Zapobiega kradzieży danych, wykorzystując techniki masowania danych i blokowania stron
- Zapobiega dostępowi napastników do kont użytkowników i wszystkich innych na serwerach webowych, oferując precyzyjną kontrolę dostępu

Akceleracja działania aplikacji

- Umożliwia caching, kompresję oraz inne metody optymalizacji ruchu HTTP/TCP, zapewniając szybsze działanie aplikacji
- Redukuje obciążenie i zwiększa wydajność poprzez odciążenie transakcji SSL
- Przeprowadza load balancing w warstwie 7, równoważąc obciążenia w klastrze serwerów webowych

WAF oferuje ekonomię skali, jaką zapewnia wirtualizacja i może być wdrażany w formie wirtualnego appliance w prywatnych chmurach, opartych na rozwiązaniach VMware bądź Microsoft Hyper-V, albo w środowiskach chmury publicznej AWS lub Microsoft Azure. Dzięki temu organizacje korzystają ze wszystkich zalet sprzętowego WAF, zyskując ekonomiczne i operacyjne przewagi wirtualizacji, takie jak skalowalność i elastyczność systemu, szybkość wdrażania, prostota zarządzania oraz redukcja kosztów.

Funkcje akceleracji - obejmujące: load balancing, content caching, kompresję i multipleksowanie połączeń - zwiększają wydajność chronionych serwisów webowych i znacząco ograniczają koszty transferu. Funkcjonalna konsola z intuicyjnym interfejsem webowym oferuje przegląd wszystkich monitorowanych i blokowanych działań, dostarczając m.in. informacje o stanie bazy sygnatur oraz zagrożeniach wykrytych i zablokowanych od czasu uruchomienia.

Serię WAF tworzą cztery modele o różnych możliwościach inspekcji, które można wdrażać w wielu scenariuszach i środowiskach zwirtualizowanych chmury publicznej i prywatnej.

Opcje implementacji

SonicWall WAF można wdrażać w wielu scenariuszach i środowiskach zwirtualizowanych chmury publicznej i prywatnej. Seria WAF jest przeznaczona do implementacji na następujących platformach systemowych:

1. Chmura prywatna:
   - VMware ESXi
   - Microsoft Hyper-V
2. Chmura publiczna:
   - Amazon Web Services (AWS)
   - Microsoft Azure

MOC OBLICZENIOWA MODELU		ZALECANA INSTANCJA AWS	ZALECANA INSTANCJA MS AZURE
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

**Przy wykorzystaniu procesorów serwerowych, takich jak Intel Xeon E5-2600*

Podsumowanie funkcjonalności WAF

Ochrona aplikacji webowych

- 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 (Geo, IP, URL, User)
- Custom Rules & Rule-chaining
- Custom Error response

Ochrona przed botnetami

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

Bezpieczne dostarczanie aplikacji webowych

- 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

Administrowanie

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

Monitorowanie i raportowanie

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

Platformy i licencjonowanie

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

Funkcje

Ochrona aplikacji webowych i zabezpieczenie przed botnetami	
OWASP Top 10 Protection	Ochrona aplikacji webowych przed 10 znanymi atakami opisywanymi przez Open Web Applicat ion Security Protection (OWASP), w tym: SQL Injectio n, XSS/CSRF, Web Fingerprinting itp. .
Sensitive Data Protection	Ochrona przed wyciekiem wrażliwych danych z możliwością blokowania stron zawierających dane wrażliwe oraz maskowania informacji typu PII (Personally Identifiable Information), takich jak numery kart płatniczych i ubezpieczeń społecznych
Session Management Controls	Zapewnia skuteczne zarządzanie sesjami i funkcje uwurzytelniania, zwiększając ochrone zapewnianą przez techniki autoryzacji, takie jak: One Time Password, Two -factor Authentication, Single Sign -On oraz certyfikaty klienckie
Web-Form Input Validation	Przeprowadza inspekcję i walidację żądań klientów pod kątem potencjalnego użycia złośliwego kodu, chroniąc serwery przed transakcjami, które mogłyby umożliwiać hakerom omijanie zabezpieczeń
Session Hijacking Monitoring	Wykrywa podsłuch, włamania a nawet kradzież sesji webowych, zapobiegając złośliwym działaniom napastników .
Perfect Forward Secrecy (PFS) prevention	Chroni sesje, które się odbyły, przed wykorzystaniem kluczy i haseł w przyszłości.
Ataki Deny Cross -Site Request Forgery (CSRF)	Rozpoznaje i zapobiega wysyłaniu nieuprawnionych żądań ze strony złośliwych stron webowych do aplikacji, do której użytkownik jest już zalogowany za pośrednictwem innej strony webowej .
Ataki block code injection lub remote code-inclusion	Rozpoznaje i neutralizuje ataki, które wykorzystują interfejs aplikacji webowej do systemu operacyjnego i prowadzą do wykonania szkodliwego kodu z poleceniami, takimi jak np. pobranie złośliwego oprogramowania .
Cookie Tampering Protection a nd Encryption	Ochrona przed kradzieżą cookie, zatruwaniem , błędami oraz metodą Cross -Site Cooking, wykorzystująca szyfrowanie i wyłączanie .
Rate Limiting for Custom Rules	Kontroluje szybkość, z jaką jest dopasowywana własna reguła lub łańcuch reguł w blok owaniu ataków słownikowych lub typu brute force.
Web server Fingerprint Protection	Chroni serwery webowe przed atakami fingerprinting u, identyfikującymi oprogramowanie aplikacji webowej, jego wersję i platformę, co służy hakerom do wykorzystania znanych luk w oprogramowaniu .
Web services/API protection	Zapobiega ujawnieniu wrażliwych informacji zawartych w usługach webowych i API.
CMS platform protection:	Wykorzystuje własne reguły w ramach wirtualnego łatania luk w celu neutralizowania nowych podatności znajdowanych w popularnych narzędziach CMS, takich jak WordPress, Joomla i Documentum.
Denial of Service Protection	Ograniczanie szybkości i dławienie ruc hu do aplikacji webowej w celu ochrony przed atakami Denial of Service (DoS).
Automatic Signature Updates	Okresowe automatyczne aktualizacje sygnatur wykorzystujące badania Capture Labs związane z nowymi zagrożeniami dla aplikacji webowych
Web Application Profiling	Unikalny mechanizm profilowania, który monitoruje znane legalne działania w ramach aplikacji webowej w celu ustalenia progów i automatycznego generowania reguł WAF dla tej aplikacji . Umożliwia użycie zaufanych adresów IP przy ustalani u progów.
Custom Rules & Error Response	Możliwość tworzenia reguł własnych w oparciu o specyficzną logikę aplikacji oraz ustalania łańcuchów reguł dla logiki seryjnej . Dostosowywalne strony blokowania oraz komunikaty błędów w przypadku egzekucji ustalonych reguł.
Botnet Filtering & Remediation	Filtrowanie botnetów na podstawie lokalizacji geograficznej, określonych adresów/zakresów IP oraz wykorzystania wbudowanej integracji z funkcją threat intelligence . Zapewnia przeciwdziałanie przy użyciu kodów captcha dla każdego typu filtra botnetów . Obsługuje także tworzenie białych i czarnych list .

Bezpieczne dostarczanie aplikacji	
Secure Web Application Offloading	Wdrażana jako Reverse Proxy do odciążania front -endu aplikacji . Obejmuje także możliwość auto-wylogowywania sesji użytkownika po określonych okresach braku aktywności.
SSL Inspection	Wbudowana obsługa zarówno ruchu HTTP, jak i SSL/TLS , ze zdolnością do przyjmowania ruchu SSL/TLS i przekazywania jako http do aplikacji webowej. Możliwość import owania i przechowywania certyfikatów SSL, z obsługą pośredniczenia w zadaniach CRS (Certificate Signing Requests) i walidacji CRL.
Stacked Authentication	Wsparcie przy wprowadzaniu rozszerzonego uwierzytelniania przed aplikacją przy użyciu metod wieloskładnikowych (multi-factor authentication) lub wymuszonego uwierzytelniania dla nie obsługiwanych aplikacji webowych
Layer-7 Load Balancing	Łatwy w użyciu l oad-balancing z utrzymywaniem sesji , dostosowywalną logiką oraz obsługą funkcji, który zapewni a także monitorowanie kondycji aplikacji webowej .
Web Application Acceleration	Wykorzystuje kombinację cachingu i kompresowania treści wraz z optymalizacją pasma sieciowego w celu zapewnienia szybszej obsługi serwisu webowego.

Zarządzanie	
Web Portal & Command Line Interface	Intuicyjny portal webowy do opartego na interfejsie graficznym administrowania – dostosowywalny wygląd obejmujący możliwość wstawiania logotypów (dla dostawców usług). Dodatkowe wsparcie dla administrowania opartego na CLI
Administrator Authenticatio n	Wsparcie dla wielu form uwierzytelniania administratora, w tym uwierzytelnianie przy użyciu MS Active Directory, LDAP, RADIUS i certyfikatów. Obejmuje wymuszanie złożonych haseł i oparte na rolach uwierzytelnianie.
Software Updates	Automatyczne aktualizacje oprogramowania z SonicWall Cloud, które są pobierane i stosowane na wszystkich licencjonowanych platformach WAF.

Monitorowanie i raportowanie	
Logging & Alerting	Granularne rejestrowanie dla zdarzeń bezpieczeństwa, systemowych i audytowych z zapewnieniem elastyczności w kontroli poziomów logów i konfigurowaniu transferu logów przy użyciu programu Syslog do zewnętrznych systemów, takich jak platformy SIEM. Oparte na stopniach ważności alerty o zdarzeniach przy użyciu poczty email.
System Monitoring & SNMP Support	Obszerna diagnostyka systemowa wykorzystująca tryby debugowania, z automatycznym generowaniem raportów TSR (Technical Support Reports). Wsparcie monitorowania od innych producentów przy użyciu SNMP i łatwo pobieralnych baz MIB.
Dashboards & Reports	Intuicyjny pulpit pokazujący informacje, takie jak Top Web Security & Botnet Threats, Latest Alerts oraz Web Application Health and Performance. Porównawcze pulpity dla stanu globalnych zagrożeń ze wsparciem Capture Labs. Raporty do pobrania w formacie PDF

Platformy i licencje	
Platformy	WAF jest dostarczany jako wirtualne appliance, które może być wdrażane w chmurze prywatnej z wirtualizatorami VMWare oraz MS Hyper-V, a także w chmurach publicznych AWS i MS Azure. W przypadku platform AWS i Azure obsługiwane są modele Bring-Your-Own-License
Model licencyjny	WAF jest dostępny w formie abonamentu z prawem korzystania z usług wsparcia w trybie 24x7. Oferowane są różne modele pod względem zasobów, w formie jednorocznych i wieloletnich SKU .

Specyfikacje systemowe przy zamówieniach

WAF 200 WAF 400 WAF 800 WAF 1600				
Obsługiwana platforma	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 (transakcje/s)	6,000	12,000	24,000	48,000
Przepustowość SSL	500 Mbps	1 Gbps	2 Gbps	4 Gbps
Rekomendowane vCPUs*	2	4	8	16
Rekomendowana pamięć	4 GB	8 GB	16 GB	32 GB
Rekomendowany Storage	8 GB	8 GB	8 GB	8 GB
Rekomendowana instancja AWS	c5.large	c5.xlarge	c5.2xlarge	c5.4xlarge
Rekomendowana instancja Azure	Standard_F2s_ v2	Standard_F4s_ v2	Standard_F8s_ v2	Standard_F16s_ v2

Produkt	SKU
SonicWall WAF 200 With24x7 Support 1yr	01-SSC-4639
SonicWall WAF 200 With 24x7 Support 2y	01-SSC-4638
SonicWall WAF 200 With 24x7 Support 3y	01-SSC-4637
SonicWall WAF 400 With 24x7 Support 1y	01-SSC-6299
SonicWall WAF 400 With 24x7 Support 2y	01-SSC-4567
SonicWall WAF400 With 24x7 Support 3yr	01-SSC-6314
SonicWall WAF 800 With 24x7 Support 1y	01-SSC-4597
SonicWall WAF 800 With 24x7 Support 2y	01-SSC-6379
SonicWall WAF 800 With 24x7 Support 3y	01-SSC-6319
SonicWall WAF 1600 With 24x7 Support 1	01-SSC-4560
SonicWall WAF 1600 With 24x7 Support 2	01-SSC-4562
SonicWall WAF 1600 With 24x7 Support 3	01-SSC-4561

**W oparciu o typowe systemy serwerowe klasy enterprise. Więcej informacji w Deployment Guides*

O firmie

SonicWall od ponad 27 lat zapobiega cyberprzestępstwom, broniąc małe i średnie przedsiębiorstwa oraz korporacje na całym świecie. Połączony potencjał produktów i partnerów tworzy ochronę w czasie rzeczywistym, dostosowaną do indywidulanych potrzeb ponad 500 tys. firm z przeszło 150 krajów. Z SonicWall można bez obaw rozwijać swój biznes.

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

Datasheet-WebAppFirewall-US-KJ-MKTG2273

SONICWALL