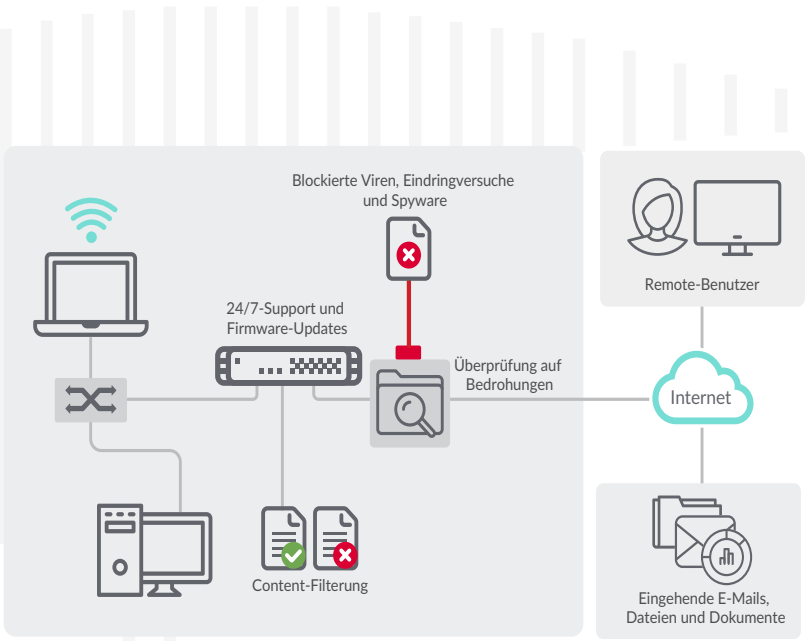
SonicWall Protection Services Suites

Netzwerkschutz und Firewall-Management
in einem einzigen integrierten Paket

Die Schaffung und Verwaltung einer effektiven Netzwerksicherheit ist eine anspruchsvolle und komplexe Aufgabe, die viel Erfahrung und Know-how erfordert. Zum Glück gibt es eine einfache Lösung, um hoch entwickelte Angriffe zu blockieren, das Firewall-Management zu vereinfachen sowie Risiken zu bewerten und zu minimieren.

SonicWall stellt eine große Vielzahl von Netzwerksicherheitslösungen in Form kostengünstiger und flexibler Pakete zur Verfügung: Threat Protection Services Suite, Essential Protection Services Suite und Advanced Protection Services Suite.



VORTEILE

- Umfassende Netzwerksicherheitslösung
- ICSA-zertifizierter Gateway-Anti-Virus- und Anti-Spyware-Schutz
- Cloudbasierter Network Security Manager
- Comprehensive Anti-Spam Service
- Hochmoderne IPS-Technologie
- Application-Intelligence und Anwendungs-kontrolle
- DNS-Sicherheit
- Content-Filterung
- 24/7-Support mit Firmware-Updates und Hardware-Austausch
- Multi-Engine-Netzwerk-Sandbox mit der patentierten Real-Time Deep Memory Inspection(RTDMI™)-Technologie von SonicWall

ICSA labs CERTIFIED ENTERPRISE FIREWALL
ICSA labs CERTIFIED ANTI-VIRUS
ICSA labs CERTIFIED ADVANCED THREAT DEFENSE
ICSA labs CERTIFIED ANTI-MALWARE

DATENBLATT

Funktionen und Vorteile

Die Threat-Protection-Services schützen Ihr Netzwerk vor Viren, Eindringlingen, Botnets, Spyware, Trojanern, Würmern und anderen bösartigen Angriffen. Die SonicWall-Firewalls und die Capture-Cloud-Datenbank werden automatisch mit wirkungsvollen Signatur-Updates versorgt, sobald neue Bedrohungen identifiziert werden – in vielen Fällen sogar bevor Softwarehersteller Sicherheitspatches für ihre Produkte bereitstellen können. Die Firewalls sind mit der patentierten RTDMI™-Engine von SonicWall ausgestattet. Diese scannt unterschiedliche Anwendungstypen und Protokolle und sorgt dafür, dass Ihr Netzwerk rund um die Uhr vor internen und externen Angriffen sowie vor Anwendungsschwachstellen geschützt ist.

Der cloudbasierte **Network Security Manager (NSM)**, ein zentralisierter Multi-Tenant-Firewall-Manager, ermöglicht eine fehlerfreie und zentrale Verwaltung sämtlicher Firewall-Prozesse gemäß prüfbaren Workflows. Durch **Reporting und Analytics** können Sie die Protokolle aller Firewalls zusammenführen und miteinander vergleichen und so Bedrohungen erkennen und überwachen – alles mithilfe einer einzigen Konsole.

Der Service **Capture ATP** revolutioniert die Erkennung ausgeklügelter Bedrohungen und das Sandboxing dank einer cloudbasierten Multi-Engine-Lösung, mit der sich unbekannte Angriffe und Zero-Day-Attacken am Gateway stoppen lassen. Capture ATP wehrt Zero-Day-Angriffe ab, bevor sie in Ihr Netzwerk gelangen. Damit können Sie einen erweiterten Schutz vor den sich schnell verändernden Bedrohungen einrichten und unterschiedlichste Dateitypen analysieren.

Der ICSA-zertifizierte **Gateway-Anti-Virus**-Schutz kombiniert ein netzwerkbasiertes Anti-Malware-System und eine dynamisch aktualisierte Cloud-Datenbank mit Dutzenden Millionen Malware-Signaturen. Durch den dynamischen Spyware-Schutz wird die Installation bösartiger Spyware verhindert und die Kommunikation mit vorhandener Spyware unterbrochen.

Die **hochmoderne IPS-Technologie** überprüft den gesamten Netzwerkverkehr auf bösartige oder ungewöhnliche Muster und bietet so einen effizienten Schutz vor Würmern, Trojanern, Software-Schwachstellen und anderen Eindringlingen. Gleichzeitig werden Zuverlässigkeit und Performance des Netzwerks erhöht.

Application Intelligence and Control umfasst eine Reihe granularer und anwendungsspezifischer Regeln, mit denen sich Anwendungen klassifizieren und Sicherheitsregeln durchsetzen lassen. Damit können Administratoren arbeitsrelevante und privat genutzte Anwendungen einfach kontrollieren und verwalten.

Der **Comprehensive Anti-Spam Service** von SonicWall schützt kleine bis mittlere Unternehmen zu über 99 % vor Spam: Tatsächlich werden mehr als 80 % aller Spammails bereits am Gateway abgefangen. Dabei kommen moderne Anti-Spam-Techniken wie Adversarial-Bayesian™- und Machine-Learning-Filter zum Einsatz.

Die Content Filtering Services (CFS) unterstützen eine umfassende Filterung von Inhalten. So können Sie Internetnutzungsregeln durchsetzen und den internen Zugriff auf ungeeignete, unproduktive oder potenziell illegale Webinhalte steuern. Die reputationsbasierten **CFS 5.0** nutzen einen Reputation-Score, der das Sicherheitsrisiko einer URL über 93 Webkategorien hinweg vorhersagt.

Bei der **DNS-Filterung** werden bösartige Websites oder Anwendungen auf DNS-Ebene blockiert. So werden schädliche oder unangemessene Inhalte herausgefiltert, ohne die TLS-Entschlüsselung zu aktivieren und die Performance zu beeinträchtigen.

Die extrem sicheren **Access-Points** von SonicWall können via Cloud mit dem SonicWall Wireless Network Manager (WNM) oder über die SonicWall-Firewalls verwaltet werden. Dies ermöglicht ein einfaches Management und eine nahtlose Integration mit den Wireless-Produkten von SonicWall.

Die Integration der **Netzwerkzugriffskontrolle** mit Aruba ClearPass ermöglicht SonicWall-Kunden ein umfassendes Profiling sowie eine umfangreiche und präzise Authentifizierung und Autorisierung für Systeme und Geräte, die auf Ihre IT-Ressourcen zugreifen wollen. SonicOS bietet eine RESTful-API, die eine Integration von Aruba ClearPass als NAC-Lösung mit den SonicWall-NGFWs unterstützt. Diese Architektur verwandelt eine statische Sicherheit in eine kontextbasierte Sicherheit, was einen flexibleren und solideren Schutz sicherstellt.

Der **24/7-Support** mit Firmware-Updates und Hardware-Austausch schützt Ihr Unternehmen und Ihre SonicWall-Investition. Der Support umfasst rund um die Uhr telefonische und webbasierte Unterstützung bei der Basis-Konfiguration und der Fehlerbehebung sowie den Austausch von Hardware im Fehlerfall.

FEATURE	THREAT PROTECTION SECURITY SUITE*	ESSENTIAL PROTECTION SECURITY SUITE	ADVANCED PROTECTION SECURITY SUITE
24/7-Support	J	J	J
IPS	J	J	J
Anwendungskontrolle	J	J	J
Content Filtering Service	J	J	J
Gateway Anti-Virus	J	J	J
Grundlegende DNS-Sicherheit	J	J	J
DNS-Filterung	N	N	J
Integration der Netzwerkzugriffskontrolle (NAC) mit Aruba ClearPass	J	J	J
Wi-Fi-6-Integration	J	J	J
Deep Packet Inspection für SSL-Verkehr	J	J	J
GeoIP-Updates	J	J	J
Botnet-Service	J	J	J
Comprehensive Anti-Spam Service	N	J	J
Capture ATP – Sandboxing (statisch, RTDMI, Arbeitsspeicher, Hypervisor, Simulation)	N	J	J
NSM – Management (Cloud)	N	N	J
NSM – Reporting (Cloud) – 7-tägige Speicherung	N	N	J

* Nur für TZ 270, 370 und 470 verfügbar.

Über SonicWall

SonicWall ermöglicht eine stabile, skalierbare und nahtlose Cybersicherheit für eine extrem dezentrale Arbeitswelt, in der jeder remote, mobil und potenziell gefährdet ist. Durch die Identifizierung unbekannter Bedrohungen, moderne Echtzeit-Überwachungsfunktionen und eine herausragende Wirtschaftlichkeit hilft SonicWall großen Unternehmen, Behörden und KMUs weltweit, die Cybersicherheitslücke zu schließen. Weitere Informationen erhalten Sie unter www.sonicwall.de.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
Weitere Informationen erhalten Sie auf unserer Website.
www.sonicwall.com

Datasheet-ProtectionServiceSuites-A4-JK-9964