

Advanced Gateway Security Suite

Umfassender Netzwerkschutz in einem einzigen integrierten Paket

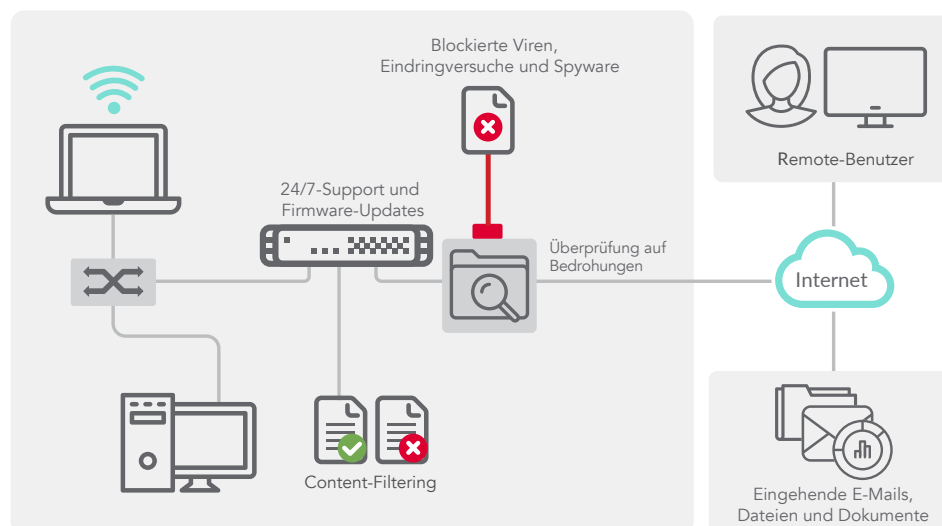
Effizienter Netzwerkschutz ist eine komplexe Aufgabe, bei der unterschiedlichste Technologien ineinandergreifen. Mit ihrem integrierten Ansatz vereinfacht die SonicWall Advanced Gateway Security Suite (AGSS) diese Herausforderung enorm. Statt die richtige Lösung aus verschiedenen isolierten Services zusammenzustellen, können Kunden alle Netzwerksicherheitsdienste, die für einen umfassenden Schutz erforderlich sind, in einem komfortablen und erschwinglichen Paket erwerben.

SonicWall AGSS ist für alle physischen und virtuellen Firewalls – einschließlich NSsp, NSa, TZ und NSv Series – verfügbar und schützt Ihr Netzwerk effizient vor Zero-Day-Attacks, Viren, Eindringversuchen, Botnets, Spyware, Trojanern, Würmern und anderen bösartigen Angriffen. Verdächtige Dateien lassen sich am Gateway in einer Cloud-basierten mehrschichtigen Sandbox prüfen, sodass Ihr Netzwerk vor unbekanntem Bedrohungen sicher bleibt. 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. Jede SonicWall-Firewall ist mit einer patentierten Reassembly-Free Deep Packet Inspection®-Engine 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. Mit der umfassenden Content-Filtering-Funktion kann Ihre SonicWall-Lösung außerdem Internetnutzungsregeln durchsetzen und den internen Zugriff auf ungeeignete, nicht arbeitsrelevante oder potenziell illegale Webinhalte steuern. Dieses leistungsstarke Servicepaket umfasst zusätzlich 24/7-Support, kritische Firmware-Updates sowie Hardware-Austausch.

Vorteile:

- Umfassende Netzwerksicherheitslösung
- ICSA-zertifizierter Gateway-Anti-Virus- und Anti-Spyware-Schutz
- Hochmoderne IPS-Technologie
- Application-Intelligence und Anwendungskontrolle
- Content-Filtering
- 24/7-Support mit Firmware-Updates und Hardware-Austausch
- Multi-Engine-Netzwerk-Sandbox mit SonicWall RTDMI
- Cloudbasierte Verwaltung über eine einzige Konsole



Advanced Gateway Security Suite

NSsp 12800 (1 Jahr)
01-SSC-6591

NSsp 12400 (1 Jahr)
01-SSC-6588

NSa 9650 (1 Jahr)
01-SSC-2036

NSa 9450 (1 Jahr)
01-SSC-0414

NSa 9250 (1 Jahr)
01-SSC-0038

NSa 6650 (1 Jahr)
01-SSC-8761

NSa 5650 (1 Jahr)
01-SSC-3674

NSa 4650 (1 Jahr)
01-SSC-3493

NSa 3650 (1 Jahr)
01-SSC-3451

NSa 2650 (1 Jahr)
01-SSC-1783

TZ600 Series (1 Jahr)
01-SSC-1460

TZ500 Series (1 Jahr)
01-SSC-1450

TZ400 Series (1 Jahr)
01-SSC-1440

TZ300 Series (1 Jahr)
01-SSC-1430

NSv 1600 (1 Jahr) 01-SSC-5787

NSv 800 (1 Jahr) 01-SSC-5737

NSv 400(1 Jahr) 01-SSC-5681

NSv 300 (1 Jahr) 01-SSC-5584

NSv 200 (1 Jahr) 01-SSC-5306

NSv 100 (1 Jahr) 01-SSC-5219

NSv 50 (1 Jahr) 01-SSC-5194

NSv 25 (1 Jahr) 01-SSC-5165

NSv 10 (1 Jahr) 01-SSC-5008

Lizenzen auch für mehrere
Jahre erhältlich

Die Artikelnummern zu allen
SonicWall-Firewalls finden Sie
unter www.sonicwall.com.

Die SonicWall Advanced Gateway Security Suite bietet:

- ein Abo für den Gateway Anti-Virus, Anti-Spyware, Intrusion Prevention and Application Intelligence and Control Service
- ein Abo für den Content Filtering Service
- ein Abo für den 24/7-Support
- ein Abo für den Capture Advanced Threat Protection (ATP) Service
- ein Abo für Capture Security Center Lite

Funktionen und Vorteile

Die umfassende Netzwerksicherheitslösung bietet alles, was Sie zum Schutz vor Ransomware, Viren, Spyware, Würmern, Trojanern, Adware, Keyloggern, Malicious Mobile Code (MMC) sowie anderen gefährlichen Anwendungen und Webinhalten benötigen.

Der Capture Advanced Threat Protection (ATP) Service revolutioniert die Bedrohungserkennung und das Sandboxing dank automatisierter Problembekämpfung sowie einer Cloud-basierten Multi-Engine-Lösung, mit der sich unbekannte Angriffe und Zero-Day-Attacken am Gateway stoppen lassen.

Capture ATP umfasst die Real-Time Deep Memory Inspection (RTDMI)-Technologie von SonicWall. Diese ist in der Lage, Malware, die kein böses Verhalten zeigt oder ihre Mechanismen durch Verschlüsselungsmethoden verschleiert, zu identifizieren und zu blockieren. Die RTDMI-Engine zwingt Malware dazu, ihre Wirkmechanismen im Speicher offenzulegen, und nutzt präzise speicherbasierte Echtzeit-Prüfmethoden, um die in großer Zahl vorkommenden Zero-Day-Bedrohungen sowie unbekannte Malware aufzudecken und abzuwehren.

Der ICISA-zertifizierte Gateway-Anti-Virus- und Anti-Spyware-Schutz kombiniert ein netzwerkbasierendes Anti-Malware-System und eine Cloud-Datenbank mit vielen Millionen Malware-Signaturen. Dies stellt einen tief greifenden Schutz vor den neuesten und gefährlichsten Bedrohungen sicher.

Die hochmoderne IPS-Technologie überprüft den gesamten Netzwerkverkehr auf böse 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.

Mit den Content-Filtering-Funktionen lassen sich Internetnutzungsregeln durchsetzen und der Zugriff auf gefährliche und nicht arbeitsrelevante Webinhalte sperren. So wird ein hohes Maß an Sicherheit und Produktivität gewährleistet.

Der 24/7-Support mit Firmware-Updates und Hardware-Austausch schützt Ihr Unternehmen und Ihre SonicWall-Investition dank kritischen Firmware-Updates und -Upgrades, erstklassigem technischem Support, schnellem Hardware-Austausch und Onlinezugriff auf Selbsthilfe-Tools.

Mit Capture Security Center Lite können Sie über eine einzige cloudbasierte Konsole Ihre SonicWall-Implementierung verwalten und Ihre Firewall-Präferenzen sichern bzw. wiederherstellen.

Die AGSS-Services im Überblick

Multi-Engine-Sandbox, Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention, Application Intelligence and Control Service

- Die Echtzeit-Gateway-Anti-Virus-Engine prüft das System auf Viren, Würmer, Trojaner und andere Internetbedrohungen.
- Dank dynamischem Spyware-Schutz wird die Installation bössartiger Spyware verhindert und die Kommunikation mit vorhandener Spyware unterbrochen.
- Intrusion Prevention bietet effizienten Schutz vor zahlreichen netzwerkbasierenden Bedrohungen wie Würmern, Trojanern und anderem bössartigen Code.
- Application Intelligence and Control erlaubt eine Klassifizierung von Anwendungen sowie die Durchsetzung von Sicherheitsregeln.

- Die dynamisch aktualisierte Signaturrendatenbank bietet einen kontinuierlichen Schutz vor Bedrohungen.
- Die mit RTDMI ausgestattete Multi-Engine-Sandbox schützt vor unbekanntem Bedrohungen wie Zero-Day-Angriffen und Ransomware.

Capture Advanced Threat Protection (Capture ATP)

- Zero-Day-Angriffe werden blockiert, bevor sie ins Netzwerk gelangen.
- Signaturen zur Problemlösung lassen sich blitzschnell auf anderen Netzwerksicherheitsappliances implementieren.
- Erweiterter Schutz vor dynamischen Bedrohungen
- Analyse unterschiedlichster Dateitypen

Content Filtering Service (CFS)

- Umfassendes Content-Filtering ermöglicht benutzerdefinierte Kontrollen, um den internen Zugriff auf ungeeignete, nicht arbeitsrelevante oder potenziell illegale Webinhalte zu steuern.
- Website-Ratings, die im lokalen Cache der SonicWall-Firewalls gespeichert sind, ermöglichen äußerst schnelle Reaktionszeiten für häufig besuchte Websites.

- Die dynamisch aktualisierte Rating-Architektur gleicht alle angefragten Websites gegen eine Cloud-Datenbank mit Millionen URLs, IP-Adressen und Domänen ab und vergleicht anschließend alle Bewertungen mit den lokalen Sicherheitsregeln.

Content Filtering Client

- Mit Real-Time Deep Memory Inspection (RTDMI) können Sie Malware schnell und zuverlässig stoppen.
- Mit dem SonicWall Content Filtering Client lassen sich Internetnutzungsregeln auf Endpunktgeräten außerhalb der Firewallgrenze durchsetzen, um die Sicherheit und Produktivität zu steigern. Der Client ist als separater Aboservice für Windows-, Mac OS- und Chrome-Endpunkte erhältlich.

24/7-Support

- Software- und Firmware-Updates und -Upgrades bieten konstante Netzwerksicherheit und sorgen dafür, dass Ihre SonicWall-Lösung jederzeit auf dem neuesten Stand bleibt.
- Telefonischer und webbasierter Support für die Basiskonfiguration und Fehlerbehebung rund um die Uhr
- Austausch von Hardware im Fehlerfall

- Jahresabo auf SonicWall-Service-Bulletins und Zugriff auf elektronische Support-Tools sowie moderierte Diskussionsforen

Capture Security Center Lite*

- Cloudbasiertes Portal
- Verwaltung über eine einzige Konsole
- Backup und Wiederherstellung von Firewall-Präferenzen

Weitere Informationen über die SonicWall Advanced Gateway Security Suite finden Sie unter www.sonicwall.com/de.

Über uns

Seit über 27 Jahren bekämpft SonicWall Cyberkriminalität, um kleinen, mittleren und großen Unternehmen weltweit Schutz zu bieten. Mit unseren Produkten und Partnern können wir eine automatisierte Echtzeitlösung zur Erkennung und Prävention von Sicherheitslücken für die individuellen Anforderungen von mehr als 500.000 Organisationen in über 215 Ländern und Regionen bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

*Für die SuperMassive 9000 Series, NSa 9250/9450/9650 und NSsp 12000 Series ist CSC Management bei Aktivierung des entsprechenden AGSS-Abos automatisch verfügbar.