



SonicWALL Content Filtering Service

Skalierbare, dynamische Lösung zum Schutz vor unerwünschten Webinhalten

- **Granulares Content Filtering**
- **Dynamisch aktualisierte Rating-Architektur**
- **Einhaltung gesetzlicher Vorschriften und Compliance Reporting**
- **Einfache webbasierte Verwaltung**
- **Leistungsstarke Web Caching- und Rating-Architektur**
- **IP-basiertes HTTPS Content Filtering**
- **Skalierbare und kosteneffiziente Lösung**

Illegale, ungeeignete und gefährliche Webinhalte können über die Webbrowser von Mitarbeitern in das Unternehmensnetzwerk gelangen. Dabei kann ungefilterter Inhalt das Netzwerk mit Malware infizieren und die Produktivität beeinträchtigen. Es besteht außerdem das Risiko, dass gesetzliche Vorschriften nicht eingehalten werden, Fördermittel entzogen werden und Haftungsprobleme auftreten. Um zum Beispiel eRate-Fördermittel zu erhalten, müssen in den USA Schulen und Bibliotheken eine Content Filtering-Lösung gemäß CIPA (Children's Internet Protection Act)-Gesetz installieren.

Der SonicWALL® Content Filtering Service (CFS) bietet Unternehmen, Bildungseinrichtungen, Bibliotheken, Behörden und öffentlichen Internet-Hotspots umfassenden Schutz vor unerwünschten Webinhalten. SonicWALL CFS blockiert ungeeignete Websites, beugt Haftungsrisiken vor und erhöht die Produktivität in großen und kleinen Organisationen. Dabei greift SonicWALL CFS auf eine umfassende Datenbank mit Millionen URLs, IP-Adressen und Websites zurück. Dank der leistungsstarken Rating- und Caching-Architektur werden Website-Ratings lokal auf den SonicWALL Network Security Appliances dynamisch aktualisiert und umgehend abgeglichen. Mit CFS können Administratoren die Zugriffsregeln auf der Grundlage von über 56 URL-Kategorien, User- bzw. Gruppen-Identitäten oder anhand der Tageszeit definieren.

Funktionen und Vorteile

Granulares Content Filtering. Erlaubt dem Administrator, alle vordefinierten Kategorien bzw. Kategoriekombinationen zu blockieren und Sicherheitsregeln gezielt anzuwenden. Um eine Anmeldung mit Benutzername und Passwort durchzusetzen kann ULA oder Single Sign-On eingesetzt werden. Mit CFS lassen sich potentiell gefährliche Inhalte, wie z. B. Java™, ActiveX® und Cookies blockieren und die Inhalte nach der Tageszeit, beispielsweise während des Unterrichts oder der Geschäftszeiten, filtern. Durch das Ausfiltern von IM-, MP3-, Freeware-, Multimedia Streaming-Anwendungen und anderer bandbreitenintensiver Dateien steigert CFS außerdem die Performance.

Dynamisch aktualisierte Rating-Architektur. Gleichet alle angefragten Websites gegen eine hochpräzise Datenbank mit Millionen klassifizierter URLs, IP-Adressen und Domänen ab. Die SonicWALL Appliances erhalten Bewertungen in Echtzeit, die anschließend mit den lokalen Sicherheitsregeln verglichen werden. Danach kann die Appliance den Zugriff anhand der lokal konfigurierten Sicherheitsregeln entweder freigeben oder sperren.

Einhaltung gesetzlicher Vorschriften und Compliance Reporting. Durch die direkte Integration mit dem mehrfach ausgezeichneten SonicWALL Global Management System (GMS) und dem SonicWALL ViewPoint™ Reporting-Paket wird die Einhaltung gesetzlicher Vorgaben unterstützt. Zusammen mit der SonicWALL ViewPoint™ Reporting Software erlaubt SonicWALL CFS eine einfache Generierung detaillierter Berichte oder grafischer Übersichtsreports, die auf Echtzeit-Informationen oder historischen Daten beruhen.

Einfache webbasierte Verwaltung. Erlaubt eine flexible Regelkonfiguration und eine umfassende Kontrolle über die Internetnutzung. Administratoren können mehrere Regeln individuell für einzelne Benutzer, Gruppen oder bestimmte Arten von Kategorien anwenden. Anhand lokaler URL-Filter können bestimmte Domänen oder Hosts freigegeben oder gesperrt werden. Um unerwünschte Inhalte effizienter zu blockieren, lassen sich außerdem individuelle Filter-Datenbanken erstellen.

Leistungsstarke Web Caching- und Rating-Architektur. Administratoren können Webseiten auf einfache Weise automatisch nach Kategorien blockieren. Dabei werden URL-Bewertungen lokal auf der SonicWALL Appliance gespeichert, so dass jeder neue Zugriff auf häufig besuchte Webseiten nur den Bruchteil einer Sekunde dauert.

IP-basiertes HTTPS Content Filtering. Erlaubt eine Zugriffskontrolle auf Websites über verschlüsseltes HTTPS. Beim HTTPS Filtering erfolgt eine Bewertung von Websites mit unerwünschten Inhalten nach Kategorien wie z. B. Glücksspiel, Shopping, Banking, Online-Aktienhandel sowie Hacking und Proxy Avoidance.

Skalierbare und kosteneffiziente Lösung. Kontrolliert das Filtern von Inhalten von der SonicWALL Network Security Appliance aus, ohne dass zusätzliche Kosten für die Hardware bzw. für die Implementierung eines separaten Filter-Servers anfallen.

Technische Daten

SonicWALL Content Filtering Service-Architektur

Der SonicWALL Content Filtering Service (CFS) wird über eine intuitive Oberfläche verwaltet und erlaubt Content Filtering und Kontrolle direkt im LAN, WLAN oder VPN. Kombiniert mit den leistungsstarken und skalierbaren SonicWALL Network Security Appliances und den umfassenden Berichts- und Verwaltungsfunktionen des SonicWALL Global Management Systems bietet CFS eine integrierte, anwenderfreundliche, leicht verwaltbare Filtering-Lösung für große und kleine Organisationen.



SonicWALL Content Filtering Service

Premium Business Edition für NSA E7500 (1 Jahr)
01-SSC-7329

Premium Business Edition für NSA E6500 (1 Jahr)
01-SSC-7330

Premium Business Edition für NSA E5500 (1 Jahr)
01-SSC-7331

Premium Business Edition für NSA 5000 (1 Jahr)
01-SSC-7330

Premium Business Edition für NSA 4500 (1 Jahr)
01-SSC-7346

Premium Business Edition für NSA 3500 (1 Jahr)
01-SSC-7333

Premium Business Edition für NSA 2400 (1 Jahr)
01-SSC-7334

Premium Business Edition für NSA 240-Serie (1 Jahr)
01-SSC-7335

Premium Business Edition für die TZ 210-Serie (1 Jahr)
01-SSC-7371

Premium Business Edition für die TZ 200-Serie (1 Jahr)
01-SSC-8634

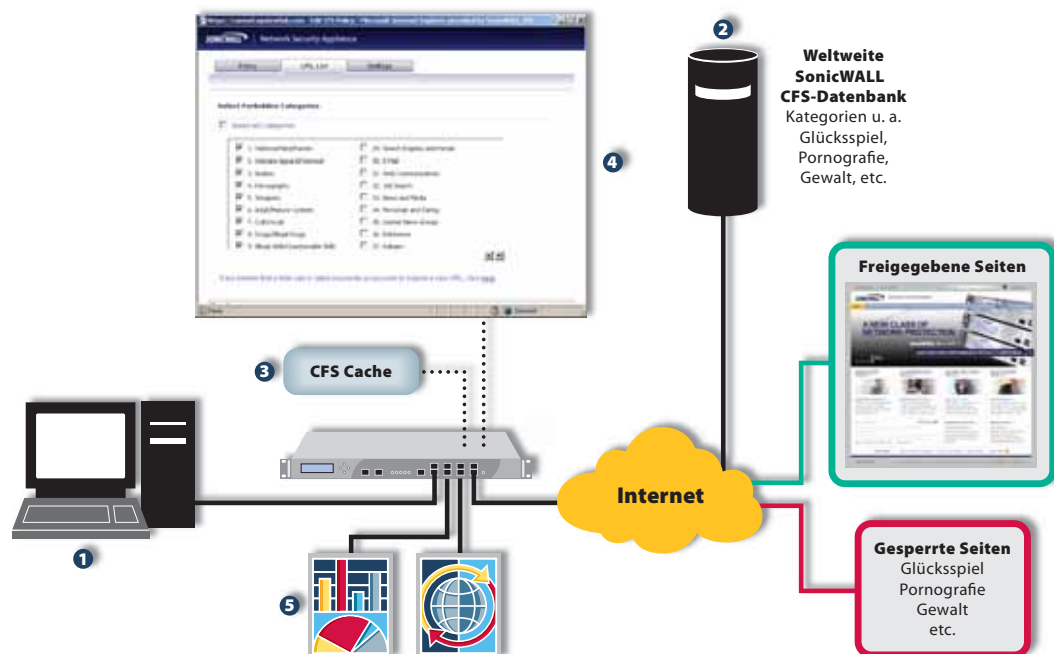
Premium Business Edition für die TZ 100-Serie (1 Jahr)
01-SSC-8637

Premium Business Edition für die TZ 180- und TZ 190-Serie (1 Jahr)
01-SSC-5650

Standard Edition für die TZ 180- und TZ 190-Serie, ohne Node-Beschränkung (1 Jahr)
01-SSC-5505

Standard Edition für TZ 180, 10/25 Nodes (1 Jahr)
01-SSC-7171

Content Filtering Service-Lizenzen auch für mehrere Jahre erhältlich.



- 1 SonicWALL CFS-Benutzer
- 2 Verteilte SonicWALL CFS-Rating-Datenbank
- 3 Lokaler Rating-Speicher für zulässige Seiten
- 4 Definition von URL-Regeln, um unerwünschte oder produktivitätshemmende Websites zu blockieren
- 5 Mit SonicWALL ViewPoint oder GMS generierte Berichte

Funktionen	CFS Premium	CFS Standard
Kategorien	56	12
User-/Gruppen-Regeln	Ja**	Nein
Dynamisches Rating	Ja	Nein
Reporting	ViewPoint*	ViewPoint*
Website Caching	Ja	Ja
Anwendung von Safe Search	Ja***	Nein
Anwendung von CFS-Regeln nach IP-Bereich	Ja***	Nein

*ViewPoint separat erhältlich. ** SonicOS Enhanced erforderlich. ***SonicOS 5.2 oder höher erforderlich.

Verfügbar für	CFS Premium	CFS Standard
TZ 180/180W	Ja	Ja
TZ 190/190W	Ja	Ja
TZ 100/100W	Ja	Nein
TZ 200/200W	Ja	Nein
TZ 210/210W	Ja	Nein
NSA-Serie	Ja	Nein
E-Class NSA-Serie	Ja	Nein

Weitere Informationen über den Content Filtering Service von SonicWALL und unser gesamtes Angebot an Sicherheitslösungen erhalten Sie auf unserer Website unter <http://www.sonicwall.com/de>.

SonicWALL Deutschland
Tel.: +49 89 4545 946
www.sonicwall.de

SonicWALL Schweiz
Tel.: +41 44 810 31 35
www.sonicwall.ch

SonicWALL Österreich
Tel.: +41 44 810 31 35
www.sonicwall.at

