

SonicWALL Content Filtering Service

FIREWALL

Skalierbare, dynamische Lösung zum Schutz vor unerwünschten Webinhalten

Mit einem Browser kann heute jeder Netzwerknutzer auf illegale oder anstößige Websites zugreifen. Diese Inhalte beeinträchtigen nicht nur die Produktivität der Mitarbeiter, sondern gefährden auch die Organisation. Dabei geht es mehr als nur um Malware, die zum Abschöpfen vertraulicher Daten genutzt werden kann. Es drohen gleichzeitig Probleme wegen der Nichteinhaltung von Vorschriften, strafrechtliche Konsequenzen oder der Verlust von Fördermitteln. So verlangen beispielsweise die US-Behörden, dass Schulen und Universitäten, die Zuschüsse für die Internet-Nutzung erhalten, eine CIPA (Children's Internet Protection Act)-konforme Content Filtering-Lösung installieren.

Der SonicWALL® Content Filtering Service (CFS) bietet Unternehmen, Bildungseinrichtungen, Bibliotheken, Behörden und öffentlichen Internet-Hotspots umfassenden Schutz vor unerwünschten Webinhalten. SonicWALL CFS ist als Abo-Service für sämtliche SonicWALL TZ-, Network Security Appliance (NSA)- oder E-Class NSA-Firewalls sowie als Bestandteil der Comprehensive Gateway Security Suite oder als TotalSecure-Abo erhältlich und 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 Firewalls dynamisch aktualisiert und umgehend abgeglichen. Mit CFS können Administratoren die Zugriffsregeln auf der Grundlage von über 59 URL-Kategorien, User- bzw. Gruppen-Identitäten oder anhand der Tageszeit definieren.

Funktionen und Vorteile

Granulares Content Filtering. Erlaubt dem Administrator, Webinhalte aller vordefinierten Kategorien bzw. Kategoriekombinationen zu blockieren bzw. die verfügbare Bandbreite zu beschränken. Um eine Anmeldung mit Benutzername und Passwort durchzusetzen kann ULA (User Level Authentication) 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 Firewalls 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. SonicWALL ViewPoint erlaubt eine einfache Generierung detaillierter Berichte oder grafischer Übersichtsreports, die auf Echtzeit-Informationen oder historischen CFS-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-Firewall 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 Firewall aus, ohne dass zusätzliche Kosten für die Hardware bzw. für die Implementierung eines separaten Filter-Servers anfallen.

- 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

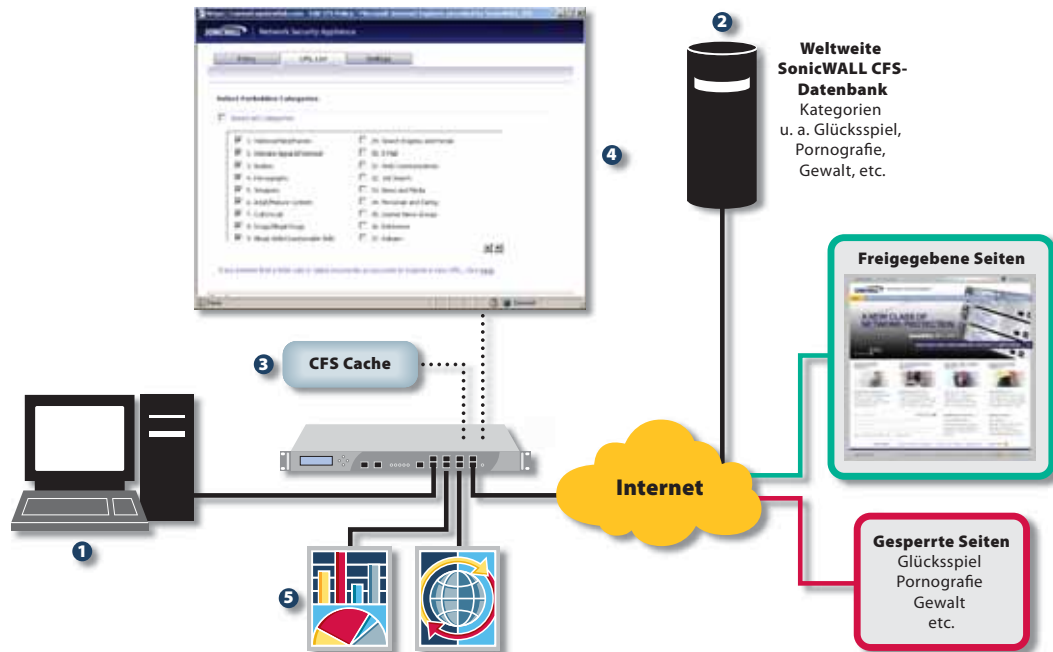
SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

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.



- 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 unproduktiver Websites zu blockieren
- 5 Mit SonicWALL ViewPoint oder GMS generierte Berichte

Funktionen	CFS Premium
Kategorien	59
User-/Gruppen-Regeln	Ja
Dynamisches Rating	Ja
Reporting	ViewPoint*
Website Caching	Ja
Anwendung von Safe Search	Ja
Anwendung von CFS-Regeln nach IP-Bereich	Ja

*ViewPoint separat erhältlich

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

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 Content Filtering Service

NSA E8500 (1 Jahr)
01-SSC-8943

NSA E7500 (1 Jahr)
01-SSC-7329

NSA E6500 (1 Jahr)
01-SSC-7330

NSA E5500 (1 Jahr)
01-SSC-7331

NSA 4500 (1 Jahr)
01-SSC-7346

NSA 3500 (1 Jahr)
01-SSC-7333

NSA 2400 (1 Jahr)
01-SSC-7334

NSA 240-Serie (1 Jahr)
01-SSC-7335

TZ 210-Serie (1 Jahr)
01-SSC-7371

TZ 200-Serie (1 Jahr)
01-SSC-8634

TZ 100-Serie (1 Jahr)
01-SSC-8637

TZ 180- und TZ 190-Serie (1 Jahr)
01-SSC-5650

Content Filtering Service-Lizenzen
auch für mehrere Jahre erhältlich

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

SonicWALL-Lösungen für dynamische Sicherheit



NETWORK SECURITY



SECURE REMOTE ACCESS



WEB & E-MAIL SECURITY



BACKUP & RECOVERY



POLICY & MANAGEMENT

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™