

Content Filtering Service und Content Filtering Client

Leistungsstarke Sicherheits- und Produktivitätslösung zum Blockieren gefährlicher und unproduktiver Webinhalte

Bildungseinrichtungen, Unternehmen und Behörden gehen heute ein erhebliches Risiko ein, wenn sie ihren Schülern, Studenten und Mitarbeitern IT-verwaltete Computer zur Verfügung stellen, die einen Zugriff auf das Internet ermöglichen. Dies gilt selbst, wenn sich der PC hinter der Firewallgrenze befindet, also dort, wo die Webnutzungsregeln der Organisation durchgesetzt werden. Besonders heikel ist es, wenn Websites mit anstößigen, illegalen oder gefährlichen Inhalten oder Bildern aufgerufen werden. Diese Sites könnten auch mit Malware infiziert sein, die unabsichtlich heruntergeladen und von Hackern zum Stehlen vertraulicher Informationen genutzt wird.

Vor allem Schulen tragen eine besondere Verantwortung, ungeeignete und jugendgefährdende Inhalte von Kindern und Jugendlichen fernzuhalten. Um eRate-Fördermittel zu erhalten, müssen in den USA Schulen und Bibliotheken eine Content-Filtering-Lösung gemäß CIPA (Children's Internet Protection Act)-Gesetz installieren. Im Fall von Unternehmen und Behörden begünstigt ein uneingeschränkter Internetzugang für Mitarbeiter privates Surfen während der Arbeitszeit, was zu enormen Produktivitätsverlusten führt und auch rechtliche Probleme nach sich ziehen kann.

In Kombination mit den SonicWall Unified Threat Management- und Next-Generation-Firewalls ist der SonicWall Content Filtering Service (CFS) eine leistungsstarke Sicherheits- und Produktivitätslösung, die eine zuverlässige und effiziente Filterung von Webinhalten in Bildungseinrichtungen, Unternehmen, Bibliotheken und Behörden erlaubt. Mit SonicWall CFS können Organisationen den Internetkonsum von Schülern, Studenten und Mitarbeitern kontrollieren, wenn sie ihre von der IT verwalteten Computer hinter der Firewall nutzen.

SonicWall CFS gleicht die aufgerufenen Websites gegen eine umfangreiche Cloud-Datenbank mit Millionen bewerteter URLs, IP-Adressen und Websites ab. Administratoren können Regeln erstellen und anwenden, um den Zugriff auf Sites basierend auf der Nutzer- oder Gruppenidentität bzw. nach Tageszeit für über 56 vordefinierte Kategorien zu erlauben oder zu verweigern. Mit CFS können außerdem Website-Ratings im lokalen Cache der SonicWall-Firewall dynamisch zwischengespeichert werden, was äußerst schnelle Reaktionszeiten ermöglicht.

Bei Laptops, die außerhalb der Firewallgrenzen verwendet werden, blockiert der SonicWall Content Filtering Client gefährliche und nicht arbeitsrelevante Webinhalte und gewährleistet so ein hohes Maß an Sicherheit und Produktivität. Der Client wird durch die SonicWall-Firewall automatisch implementiert und bereitgestellt. Damit können IT-Administratoren den webbasierten Zugang für Roaming-Geräte kontrollieren. Zudem lässt sich der Content Filtering Client so konfigurieren, dass die internen Richtlinien automatisch angewendet werden, sobald das Gerät wieder mit der Netzwerkfirewall verbunden ist. Verwalten und überwachen lässt sich der Client über eine leistungsstarke Regel- und Berichts-Engine in der Cloud, die über die Firewall-Oberfläche zugänglich ist. Sollte ein veralteter Client versuchen, über eine Verbindung zum internen Netzwerk auf das Internet zuzugreifen, wird der Zugriff verweigert und der Nutzer erhält eine Mitteilung mit Hinweisen zur Behebung des Problems.

Funktionen und Vorteile

Granulares Content-Filtering erlaubt dem Administrator, Webinhalte

Vorteile:

- Best-in-Class-Sicherheit
- Granulares Content-Filtering
- Dynamisch aktualisierte Rating-Architektur
- Analyse des Anwendungsverkehrs
- Einfache webbasierte Verwaltung
- Leistungsstarke Web-Caching- und Rating-Architektur
- IP-basiertes HTTPS-Content-Filtering
- Skalierbare, kosteneffiziente Lösung
- Content Filtering Client für Roaming-Geräte

SonicWall Content Filtering Service	
NSsp 12800 (1 Jahr)	01-SSC-7850
NSsp 12400 (1 Jahr)	01-SSC-7698
NSa 9650 (1 Jahr)	01-SSC-2136
NSa 9450 (1 Jahr)	01-SSC-1158
NSa 9250 (1 Jahr)	01-SSC-0331
NSa 6650 (1 Jahr)	01-SSC-8972
NSa 5650 (1 Jahr)	01-SSC-3692
NSa 4650 (1 Jahr)	01-SSC-3583
NSa 3650 (1 Jahr)	01-SSC-3469
NSa 2650 (1 Jahr)	01-SSC-1970
TZ600 Series (1 Jahr)	01-SSC-0234
TZ500 Series (1 Jahr)	01-SSC-0464
TZ400 Series (1 Jahr)	01-SSC-0540
TZ300 Series (1 Jahr)	01-SSC-0608
SOHO Series (1 Jahr)	01-SSC-0676
NSv 1600 (1 Jahr)	01-SSC-5801
NSv 800 (1 Jahr)	01-SSC-5774
NSv 400 (1 Jahr)	01-SSC-5690
NSv 300 (1 Jahr)	01-SSC-5649
NSv 200 (1 Jahr)	01-SSC-5335
NSv 100 (1 Jahr)	01-SSC-5238
NSv 50 (1 Jahr)	01-SSC-5203
NSv 25 (1 Jahr)	01-SSC-5177
NSv 10 (1 Jahr)	01-SSC-5129

SonicWall Content Filtering Client	
5 Benutzer (1 Jahr)	01-SSC-1222
10 Benutzer (1 Jahr)	01-SSC-1252
25 Benutzer (1 Jahr)	01-SSC-1225
50 Benutzer (1 Jahr)	01-SSC-1228
100 Benutzer (1 Jahr)	01-SSC-1231
250 Benutzer (1 Jahr)	01-SSC-1255
500 Benutzer (1 Jahr)	01-SSC-1237
750 Benutzer (1 Jahr)	01-SSC-1240
1.000 Benutzer (1 Jahr)	01-SSC-1243
2.000 Benutzer (1 Jahr)	01-SSC-1246
5.000 Benutzer (1 Jahr)	01-SSC-1249

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 (SSO) eingesetzt werden. Mit CFS lassen sich potenziell gefährliche Inhalte wie z. B. Java™, ActiveX® und Cookies blockieren und die Inhalte nach Tageszeit, beispielsweise während der Unterrichts- oder Geschäftszeiten, filtern. Durch das Ausfiltern von IM-, MP3-, Freeware- und Streaming-Media-Anwendungen sowie anderen bandbreitenintensiven Dateien steigert CFS außerdem die Performance.

Für den Content Filtering Service und Content Filtering Client sind auch Mehrjahreslizenzen erhältlich.

Weitere Informationen über die Content Filtering-Lösungen von SonicWall und unser gesamtes Angebot an Sicherheitslösungen erhalten Sie auf unserer Website unter www.sonicwall.com/de.

Eine dynamisch aktualisierte Rating-Architektur gleicht alle aufgerufenen 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.

Die Application Traffic Analytics-Suite beinhaltet SonicWall Capture Security Center, das SonicWall Global Management System (GMS®) und SonicWall Analyzer. Diese bieten einen Einblick in aktuelle und historische Analysen der über die Firewall übermittelten Daten, einschließlich der blockierten und besuchten Websites nach Benutzer.

Die 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 und nicht arbeitsrelevante Inhalte effizienter zu blockieren, lassen sich außerdem Filterlisten erstellen bzw. individuell anpassen.

Mithilfe der leistungsstarken Web-Caching- und Rating-Architektur können Administratoren Websites auf einfache Weise automatisch nach Kategorien blockieren. Dabei werden URL-Bewertungen lokal auf der SonicWall-Firewall gespeichert, sodass 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 oder unproduktiven Bildern und Inhalten nach Kategorien (z. B. Gewalt, Hass, Onlinebanking, Shoppen).

Die 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.

Content-Filtering Client für Roaming-Geräte. Erweitert die Durchsetzung interner Webnutzungsregeln, sodass bei Geräten außerhalb der Firewallgrenzen unerwünschte und unproduktive Inhalte blockiert werden. Jedes Mal, wenn das Gerät eine Verbindung zum Internet herstellt, setzt der Client Sicherheits- und Produktivitätsregeln durch – unabhängig davon, wo die Verbindung aufgebaut wird.

Architektur der SonicWall Content Filtering-Lösungen

Der SonicWall Content Filtering Service wird über eine SonicWall-Firewall bereitgestellt und verwaltet. IT-Administratoren können Internetnutzungsregeln erstellen und durchsetzen und auf diese Weise verhindern, dass IT-verwaltete Endpunktgeräte hinter der Firewall über ein LAN, Wireless LAN oder

VPN auf unerwünschte und unproduktive Websites zugreifen.

Bei Roaming-Geräten, die sich außerhalb der Firewallgrenzen befinden, wendet der SonicWall Content Filtering Client die Sicherheits- und Produktivitätsregeln an, sobald das Gerät eine Verbindung zum Internet herstellt – unabhängig davon, wo die Verbindung aufgebaut wird. Vereinfacht wird die Implementierung durch die Enforcement-Funktionen einer SonicWall-Firewall. Der Client wird über eine leistungsstarke Regel- und Berichts-Engine verwaltet und überwacht.

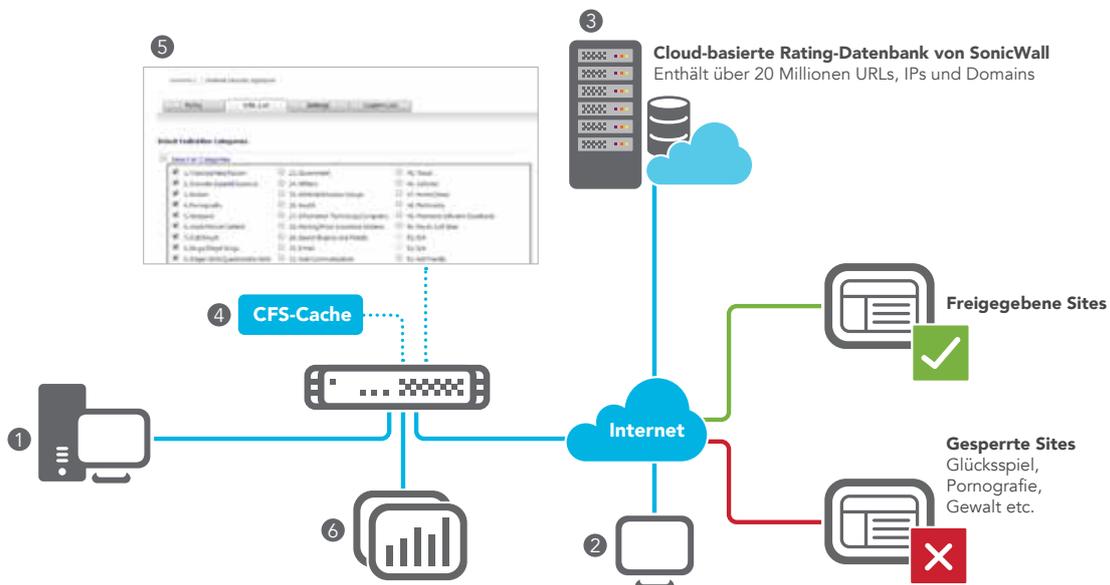
Mit SonicWall Analyzer, SonicWall Capture Security Center oder GMS können IT-Administratoren aktuelle und historische Berichte zur Internetnutzung erstellen.

Über uns

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehr für die individuellen Anforderungen von über 500.000 Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

	Content Filtering Service Premium	Content Filtering Client
Kategorien	56 und mehr	56 und mehr
User-/Gruppen-Regeln	✓	✓
Dynamisches Rating	✓	✓
Reporting	Analyzer*, Capture Security Center* und GMS*	✓
Website-Caching	✓	✓
Anwendung von Safe Search	✓	✓
Anwendung von CFS-Regeln nach IP-Bereich	✓	✓
Verfügbar für: <ul style="list-style-type: none"> • TZ Series • NSa Series • NSsp Series 	<ul style="list-style-type: none"> ✓ ✓ ✓ 	Über eine SonicWall-Firewall bereitgestellte Endpunktgeräte mit Windows, Chrome OS oder Mac OS
YouTube für Schulen	✓	✓
HTTPS-Content-Filtering	✓	✓
Filterung nach Zeitplan	✓	✓
Content-Filtering-Datenbank	Dynamisch aktualisierte Datenbank mit über 20 Millionen URLs, IPs und Domains	
Unterstützte Firmwareversionen/ Betriebssysteme	SonicOS 5.x und höher	Firewall – 5. Generation: SonicOS 5.9.0.4 und höher, 6. Generation: SonicOS 6.1.1.6 und höher; Laptop – Microsoft Windows 7/8/10/Windows Server 3/Server 8/Server 12, Chrome OS, Mac OS 10.8 und höher

*Analyzer, Capture Security Center und GMS sind optional und separat erhältlich.



1. SonicWall CFS-Nutzer hinter der Firewall
2. Roaming CF Client-Nutzer außerhalb der Firewallgrenze
3. Verteilte SonicWall CFS Rating-Datenbank
4. Lokaler Rating-Speicher für zulässige Sites
5. Definition von URL-Regeln, um unerwünschte oder unproduktive Websites zu blockieren
6. Mit SonicWall Analyzer, Capture Security Center oder GMS erstellte aktuelle und historische Berichte

SonicWall, Inc.

1033 McCarthy Boulevard | Milpitas, Kalifornien 95035, USA
 Weitere Informationen erhalten Sie auf unserer Website.

www.sonicwall.com

© 2018 SonicWall Inc. ALLE RECHTE VORBEHALTEN. SonicWall ist eine Marke oder eingetragene Marke von SonicWall Inc. und/oder deren Tochtergesellschaften in den USA und/oder anderen Ländern. Alle anderen Marken und eingetragenen Marken sind Eigentum der jeweiligen Inhaber.

Datasheet-ContentFilteringService-US-VG-MKTG2926

SONICWALL®