Content Filtering Service und Content Filtering Client

Leistungsstarke Sicherheits- und Produktivitätslösung zum Blockieren gefährlicher und unproduktiver Webinhalte

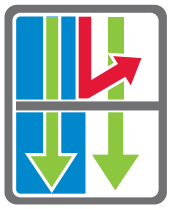
Bildungseinrichtungen, Unternehmen und Behörden gehen heute ein erhebliches Risiko ein, wenn sie ihren Schülern, Studenten und Mitarbeitern IT-verwaltete Computer zur Verfügung stellen, die einen Zugriff auf das Internet ermöglichen. Dies gilt selbst, wenn sich der PC hinter der Firewallgrenze befindet, 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 E-Rate-Fördermittel zu erhalten, müssen Schulen und Bibliotheken in den USA eine Content-Filtering-Lösung gemäß CIPA(Children's Internet Protection Act)-Gesetz installieren. Im Fall von Unternehmen und Behörden begünstigt ein uneingeschränkter Internetzugriff 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.



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

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 (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.

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 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 zwischengespeichert, sodass jeder neue Zugriff auf häufig besuchte Websites 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.

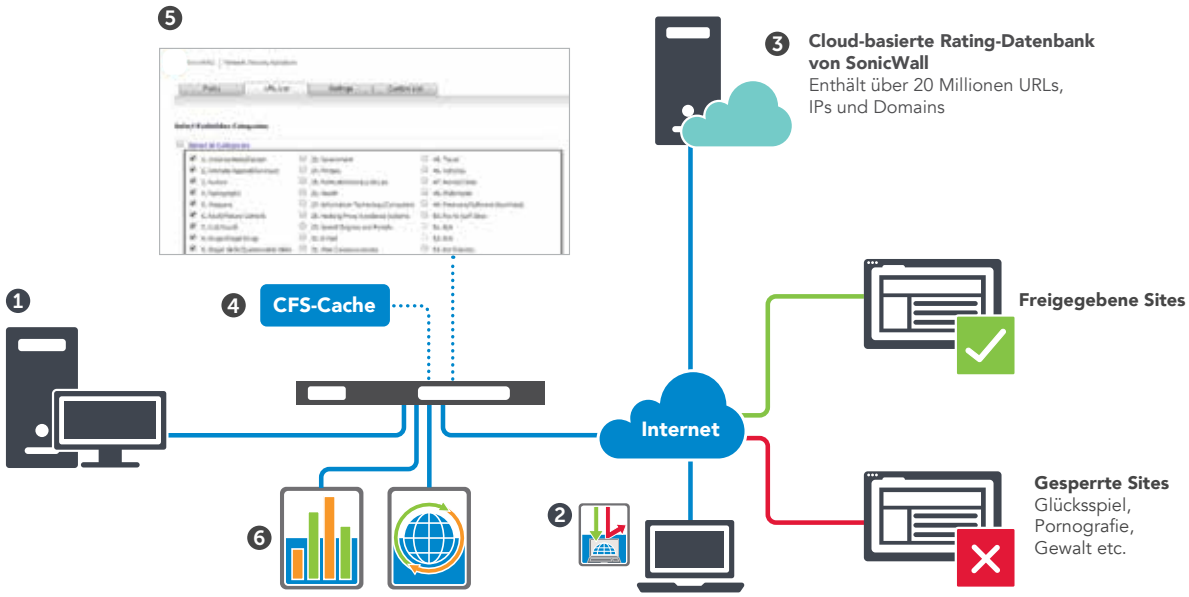
Der Content-Filtering Client für Roaming-Geräte erweitert die Durchsetzung interner Webnutzungsregeln, sodass bei Geräten außerhalb der Firewallgrenzen unerwünschte und unproduktive Inhalte blockiert werden. Jedes Mal, wenn das Gerät eine Verbindung zum Internet herstellt, setzt der Client Sicherheits- 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 oder dem SonicWall Global Management System (GMS) können IT-Administratoren aktuelle und historische Berichte zur Internetnutzung erstellen.



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 oder GMS erstellte aktuelle und historische Berichte

Funktionen

	Content Filtering Service Premium	Content Filtering Client
Kategorien	> 56	> 56
User-/Gruppen-Regeln	Ja	Ja
Dynamisches Rating	Ja	Ja
Reporting	Analyzer* und GMS*	Ja
Website-Caching	Ja	Ja
Anwendung von Safe Search	Ja	Ja
Anwendung von CFS-Regeln nach IP-Bereich	Ja	Ja
Verfügbar für: • TZ Series • NSA Series • E-Class NSA Series • SuperMassive 9000 Series • SuperMassive E10000 Series	Ja Ja Ja Ja Ja	Endpunktgeräte mit Windows, Chrome OS oder Mac OS. Bereitstellung über eine SonicWall-Firewall.
YouTube für Schulen	Ja	Ja
HTTPS-Content-Filtering	Ja	Ja
Filterung nach Zeitplan	Ja	Ja
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 und GMS sind optional und separat erhältlich.*

Über SonicWall

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access-Security über Netzwerksicherheit bis zu E-Mail-Security: Wir haben unser Produktportfolio kontinuierlich weiterentwickelt, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein. www.sonicwall.com

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.

SonicWall Content Filtering Service	
SuperMassive E10800 (1 Jahr)	01-SSC-9557
SuperMassive E10400 (1 Jahr)	01-SSC-9539
SuperMassive E10200 (1 Jahr)	01-SSC-9531
SuperMassive 9800 (1 Jahr)	01-SSC-0821
SuperMassive 9600 (1 Jahr)	01-SSC-4112
SuperMassive 9400 (1 Jahr)	01-SSC-4148
SuperMassive 9200 (1 Jahr)	01-SSC-4184
NSA E8500 (1 Jahr)	01-SSC-8943
NSA 6600 (1 Jahr)	01-SSC-4222
NSA 5600 (1 Jahr)	01-SSC-4246
NSA 4600 (1 Jahr)	01-SSC-4417
NSA 3600 (1 Jahr)	01-SSC-4441
NSA 2600 (1 Jahr)	01-SSC-4465
NSA 250M Series (1 Jahr)	01-SSC-4576
NSA 220 Series (1 Jahr)	01-SSC-4618
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

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

SonicWall
5455 Great America Parkway, Santa Clara, CA 95054
www.sonicwall.com
Informationen zu unseren Niederlassungen außerhalb Nordamerikas finden Sie auf unserer Website.

Datasheet-SonicWall-ContentFilteringService-US-VG-29434