Content Filtering Service

Leistungsstarke Sicherheits- und Produktivitätslösung zum Blockieren gefährlicher und unproduktiver Webinhalte

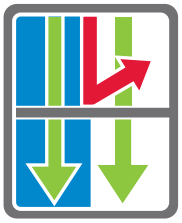
Bildungseinrichtungen, Unternehmen und Behörden gehen heute ein erhebliches Risiko ein, wenn sie ihren Schülern, Studenten und Mitarbeitern IT-verwaltete Computer zur Verfügung stellen, die einen Zugriff auf das Internet ermöglichen. Dies gilt selbst, wenn sich der PC hinter der Firewallgrenze befindet, also dort, wo die Web-nutzungsregeln der Organisation durchgesetzt werden. Besonders heikel ist es, wenn Webseiten mit anstößigen, illegalen oder gefährlichen Inhalten aufgerufen werden. Diese Seiten 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 Internetzugriff privates Surfen während der Arbeitszeit, was zu enormen Produktivitätsverlusten führt und auch rechtliche Probleme nach sich ziehen kann.

In Kombination mit den Dell SonicWALL Unified Threat Management- und Next-Generation Firewalls ist Dell™ 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 Dell SonicWALL CFS können Organisationen den Internetkonsum von Schülern, Studenten und Mitarbeitern kontrollieren, wenn sie ihre IT-verwalteten Computer hinter der Firewall nutzen.

Dell 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 Dell SonicWALL-Firewall dynamisch gespeichert werden, was äußerst schnelle Reaktionszeiten ermöglicht.

Bei Laptops, die außerhalb der Firewallgrenzen verwendet werden, blockiert der Dell SonicWALL Content Filtering Client gefährliche und nicht arbeitsrelevante Webinhalte und gewährleistet so ein hohes Maß an Sicherheit und Produktivität. Der Client wird durch die Dell 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 Firewalloberfläche 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 und 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 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- und Multimedia-Streaming-Anwendungen sowie anderen bandbreitenintensiven Dateien steigert CFS außerdem die Performance.

Dynamisch aktualisierte Rating-Architektur. Gleicht alle aufgerufenen Websites gegen eine hochpräzise Datenbank mit Millionen klassifizierter URLs, IP-Adressen und Domänen ab. Die Dell 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.

Application Traffic Analytics-Suite. Umfasst das Dell SonicWALL Global Management System (GMS®), Dell SonicWALL Analyzer und Dell SonicWALL Scrutinizer. Diese liefern einen Einblick in aktuelle und historische Analysen der über die Firewall übermittelten Daten, einschließlich der blockierten und besuchten Websites nach Benutzer.

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 individuelle Filterlisten erstellen.

Leistungsstarke Web-Caching- und Rating-Architektur. Administratoren können Webseiten auf einfache Weise automatisch nach Kategorien blockieren. Dabei werden URL-Bewertungen lokal auf der Dell SonicWALL-Firewall gespeichert, 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).

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

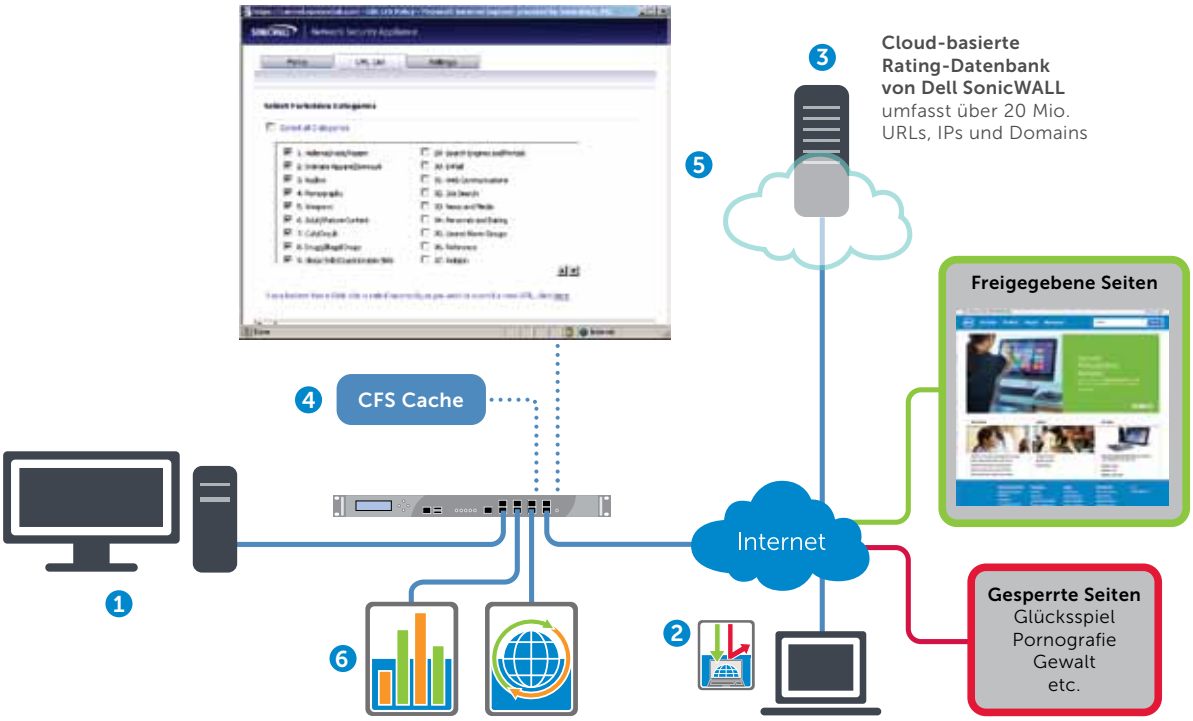
Content-Filtering Client für Roaming-Geräte. Erweitert die Durchsetzung interner Webnutzungsregeln, sodass bei Geräten außerhalb der Firewallgrenzen unerwünschte und unproduktive Inhalte blockiert werden. Jedes Mal, wenn das Gerät eine Verbindung zum Internet herstellt, setzt der Client Sicherheits-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

Architektur der Dell SonicWALL Content-Filtering-Lösung

Der Dell SonicWALL Content Filtering Service wird über eine Dell SonicWALL-Firewall bereitgestellt und verwaltet. IT-Administratoren können Internetnutzungsregeln erstellen und durchsetzen und 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 Dell 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 Dell SonicWALL-Firewall. Der Client wird über eine leistungsstarke Regel- und Berichts-Engine verwaltet und überwacht.

Mit Dell SonicWALL Analyzer oder dem Dell SonicWALL Global Management System (GMS) können IT-Administratoren aktuelle und historische Berichte zur Internetnutzung erstellen.



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

Funktionen

	CFS Premium	CF 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-Serie NSA-Serie E-Class NSA-Serie SuperMassive 9000-Serie SuperMassive E10000-Serie	 Ja Ja Ja Ja Ja	Endpunktgeräte mit Windows oder Mac OS. Bereitstellung über eine Dell 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 – Gen5: SonicOS 5.9.0.2 und höher; Gen6: SonicOS 6.1.1.6 und höher; Laptop – Microsoft Windows XP (SP2 und höher)/7/8/ Windows Server 3/Server 8/ Server 12, Mac OS 10.6 und höher

**Analyzer und GMS sind optional und separat erhältlich.*

Dell 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 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-Serie (1 Jahr)
01-SSC-4576

NSA 220-Serie (1 Jahr)
01-SSC-4618

TZ 215-Serie (1 Jahr)
01-SSC-4763

TZ 205-Serie (1 Jahr)
01-SSC-4805

TZ 105-Serie (1 Jahr)
01-SSC-4850

Dell 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

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

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

Weitere Informationen:

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
Tel.: +1 408.745.9600
Fax: +1 408.745.9300

DataSheet-CFS-A4-TD635-20140423