Content Filtering Service

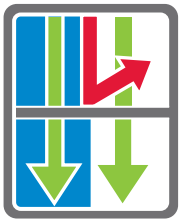
Powerful protection and productivity solution to block access to harmful and unproductive web content

Educational institutions, businesses and government agencies assume substantial risks when they provide students and employees IT-issued computers that can be used to access the Internet, even when the device is behind the firewall perimeter where organizational web use policies are enforced. This is particularly true when those connections are used to access sites containing information or images that are inappropriate, dangerous or even illegal. These sites may also be infected with malware that can be inadvertently downloaded and then used to steal confidential information.

Schools, in particular, have a responsibility to protect students from inappropriate and harmful web content. In addition, to receive eRate funding, both schools and libraries are required by law to install a content filtering solution in compliance with the Children's Internet Protection Act (CIPA). For businesses and government agencies, providing employees with uncontrolled web access can result in non-productive web surfing, creating tremendous losses in productivity, not to mention the potential for legal liability.

Dell™ SonicWALL™ Content Filtering Service (CFS) running on Dell SonicWALL Unified Threat Management and next-generation firewalls is a powerful protection and productivity solution that delivers unequalled content filtering enforcement for educational institutions, businesses, libraries and government agencies. Using Dell SonicWALL CFS, organizations have control over the web sites students and employees can access using their IT-issued computer behind the firewall. Dell SonicWALL CFS compares requested web sites against a massive database in the cloud containing millions of rated URLs, IP addresses and web sites. CFS provides administrators with the tools to create and apply policies that allow or deny access to sites based on individual or group identity, or by time of day, for over 56 pre-defined categories. CFS also dynamically caches web site ratings locally on the Dell SonicWALL firewall for near-instantaneous response times.

For laptops that are used outside the firewall perimeter, the Dell SonicWALL Content Filtering Client addresses safety, security and productivity concerns by extending the controls to block harmful and unproductive web content. The client is automatically deployed and provisioned through a Dell SonicWALL firewall. In addition to providing IT administrators the tools to control web-based access for roaming devices, the Content Filtering Client can be configured to automatically switch enforcement to the internal policy once the device reconnects to the network firewall. The client is managed and monitored using a powerful policy and reporting engine in the cloud that is accessed seamlessly from the firewall interface. In the event an outdated client attempts to connect to the internal network to access the Internet, the connection is denied and the user receives a message with steps for remediation.



Benefits:

- Best in-class protection
- Granular content filtering controls
- Dynamically updated rating architecture
- Application traffic analytics
- Easy-to-use web-based management
- High-performance web caching and rating architecture
- IP-based HTTPS content filtering
- Scalable, cost-effective solution
- Content Filtering Client for roaming devices

Features and benefits

Granular content filtering allows the administrator to block or apply bandwidth management to all pre-defined categories or any combination of categories. Administrators can apply User Level Authentication (ULA) and Single Sign-On (SSO) to enforce username and password logon. CFS can block potentially harmful content such as Java™, ActiveX®, and Cookies, as well as schedule filtering by time of day, such as during school or business hours. CFS also enhances performance by filtering out IM, MP3s, streaming media, freeware and other files that drain bandwidth.

Dynamically updated rating architecture cross-references all requested web sites against a highly accurate database categorizing millions of URLs, IP addresses and domains. The Dell SonicWALL firewall receives ratings in real time, and then compares each rating to the local policy setting. The appliance will then either allow or deny the request based on the administrator's locally configured policy.

Application traffic analytics suite includes Dell SonicWALL Global Management System (GMS®), Dell SonicWALL Analyzer and Dell SonicWALL Scrutinizer, each of which provides real-time and historic analysis of data transmitted through the firewall, including web sites blocked and visited by user.

Easy-to-use web-based management enables flexible policy configuration and complete control over Internet usage. Administrators can enforce multiple custom policies for individual users, groups or specific category types. Local URL filtering controls can allow or deny specific domains or hosts. To block objectionable and unproductive material more effectively, administrators can also create or customize filtering lists.

High-performance web caching and rating architecture allows administrators to block sites easily and automatically by category. URL ratings are cached locally on the Dell SonicWALL firewall, so that response time for subsequent access of frequently visited sites is only a fraction of a second.

IP-based HTTPS content filtering allows administrators to control user access to web sites over encrypted HTTPS. HTTPS filtering is based on the categorical rating of web sites containing information or images that are objectionable or unproductive such as violence, hate, online banking, shopping and others.

Scalable, cost-effective solution controls content filtering from the Dell SonicWALL firewall, eliminating the need for additional hardware or deployment expenditures on a separate dedicated filtering server.

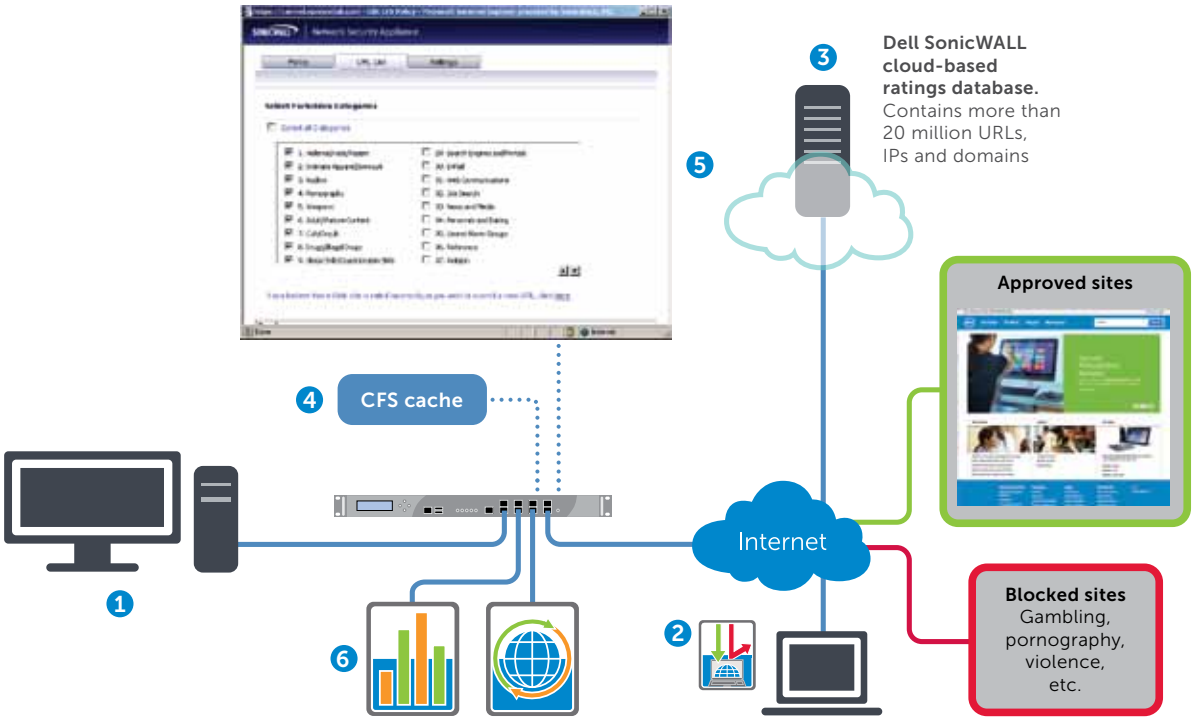
Content Filtering Client for roaming devices extends enforcement of internal web use policies to block objectionable and unproductive Internet content for devices located outside the firewall perimeter. The client enforces security and productivity policies whenever the device connects to the Internet regardless of where the connection is established.

Dell SonicWALL Content Filtering solutions architecture

Deployed and managed through a Dell SonicWALL firewall, Dell SonicWALL Content Filtering Service enables IT administrators to create and enforce Internet use policies that block IT-issued endpoint devices located behind the firewall from accessing inappropriate and unproductive web sites over a LAN, wireless LAN or VPN.

For roaming devices located outside the firewall perimeter, Dell SonicWALL Content Filtering Client extends security and productivity policies whenever the device connects to the Internet regardless of where the connection is established. Deployment is simplified using the enforcement capability of a Dell SonicWALL firewall and the client is managed and monitored using a powerful policy and reporting engine.

Using Dell SonicWALL Analyzer or Dell SonicWALL Global Management System (GMS), IT administrators can create real-time and historical reports on web usage.



1. Dell SonicWALL CFS user behind the firewall
2. Roaming CF Client user outside the firewall perimeter
3. Distributed Dell SonicWALL CFS ratings database
4. Local ratings cache of acceptable sites
5. Set URL polices to block objectionable or counter productive web sites
6. Real-time and historical reports using Dell SonicWALL Analyzer or GMS

Features

	CFS Premium	CF Client
Categories	56+	56+
User/group policies	Yes	Yes
Dynamic rating	Yes	Yes
Reporting	Analyzer* and GMS*	Yes
Web site caching	Yes	Yes
Safe search enforcement	Yes	Yes
CFS policy enforcement per IP range	Yes	Yes
Available on: TZ Series NSA Series E-Class NSA Series SuperMassive 9000 Series SuperMassive E10000 Series	 Yes Yes Yes Yes Yes	Endpoint devices running Windows or Mac OS. Deployed through a Dell SonicWALL firewall.
YouTube for Schools	Yes	Yes
HTTPS content filtering	Yes	Yes
Filter by schedule	Yes	Yes
Content Filtering database	Dynamically updated base containing over 20 millions URLs, IPs and domains	
Supported firmware versions/ operating systems	SonicOS 5.x and later	Firewall-SonicOS 5.8.1.14 and later; Laptop-Microsoft Windows XP (Service Pack 2 and above)/XP/7/8/ Windows Server 3/Server 8/Server 12, Mac OS 10.6 and later

**Analyzer and GMS are optional and sold separately.*

Dell SonicWALL Content Filtering Service

SuperMassive E10800 (1-year)
01-SSC-9557

SuperMassive E10400 (1-year)
01-SSC-9539

SuperMassive E10200 (1-year)
01-SSC-9531

SuperMassive 9600 (1-year)
01-SSC-4112

SuperMassive 9400 (1-year)
01-SSC-4148

SuperMassive 9200 (1-year)
01-SSC-4184

NSA E8500 (1-year)
01-SSC-8943

NSA 6600 (1-year)
01-SSC-4222

NSA 5600 (1-year)
01-SSC-4246

NSA 4600 (1-year)
01-SSC-4417

NSA 3600 (1-year)
01-SSC-4441

NSA 2600 (1-year)
01-SSC-4465

NSA 250M Series (1-year)
01-SSC-4576

NSA 220 Series (1-year)
01-SSC-4618

TZ 215 Series (1-year)
01-SSC-4763

TZ 205 Series (1-year)
01-SSC-4805

TZ 105 Series (1-year)
01-SSC-4850

Dell SonicWALL Content Filtering Client

5 Users (1-year)
01-SSC-1222

10 Users (1-year)
01-SSC-1252

25 Users (1-year)
01-SSC-1225

50 Users (1-year)
01-SSC-1228

100 Users (1-year)
01-SSC-1231

250 Users (1-year)
01-SSC-1255

500 Users (1-year)
01-SSC-1237

750 Users (1-year)
01-SSC-1240

1,000 Users (1-year)
01-SSC-1243

2,000 Users (1-year)
01-SSC-1246

5,000 Users (1-year)
01-SSC-1249

Multi-year Content Filtering Service and Content Filtering Client SKUs are available.

For more information on Dell SonicWALL Content Filtering solutions and our complete line of security offerings, please visit our web site at **www.sonicwall.com**.

For more information

Dell SonicWALL
2001 Logic Drive
San Jose, CA 95124

www.sonicwall.com
T +1 408.745.9600
F +1 408.745.9300

Dell Software
5 Polaris Way, Aliso Viejo, CA 92656 | www.dell.com
If you are located outside North America, you can find local office information on our Web site.

© 2013 Dell, Inc. ALL RIGHTS RESERVED. Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

DSW 527-09/13