



SonicWALL Content Filtering Service

NETWORK SECURITY

Scalable, dynamic solution to block non-productive Web content

Illegal, inappropriate and harmful Web content can enter your network via any user's browser. Unfiltered content can infect your network with malware, drain productivity, as well as put your organization at risk for regulatory non-compliance, funding withdrawal and even criminal liability. For instance, schools and libraries that receive eRate funding are required by law to install a content filtering solution in compliance with the Children's Internet Protection Act (CIPA).

SonicWALL® Content Filtering Service (CFS) provides unequalled content filtering enforcement for businesses, educational institutions, libraries and government agencies, as well as distributed public Internet hotspots. SonicWALL CFS blocks inappropriate content, reduces organizational liability and increases productivity for organizations of any size.

SonicWALL CFS utilizes a comprehensive database of millions of URLs, IP addresses and Web sites. Using a high-performance rating and caching architecture, CFS dynamically updates ratings locally on a SonicWALL network security appliance for instantaneous comparison. With CFS, administrators can apply access or denial policies based upon over 56 URL categories, individual or group identity, or time of day.

Features and Benefits

Granular content filtering allows the administrator to block all pre-defined categories or any combination of categories, and to apply these policies on a granular level. User Level Authentication (ULA) and Single sign-on (SSO) can be used 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 Web sites as they are requested against a highly accurate database categorizing millions of URLs, IP addresses and domains. The SonicWALL appliance receives ratings in real time, and then compares that rating to the local policy setting. The appliance will then either allow or deny the request, based on the administrator's locally-configured policy.

Regulatory reporting and compliance is supported by direct integration with SonicWALL's award-winning Global Management System (GMS) and SonicWALL ViewPoint™ reporting package. SonicWALL ViewPoint™ reporting software along with SonicWALL CFS can allow management to easily run detailed or "at-a-glance" graphical reports on real-time or historical data.

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 more effectively block objectionable material, administrators can also create or customize filtering databases.

High-performance Web caching and rating architecture allows administrators to easily and automatically block sites by category. URL ratings are cached locally on the SonicWALL appliance, 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 inappropriate Web site types, such as Gambling, Online Banking, Online Brokerage and Trading, Shopping and Hacking/Proxy Avoidance.

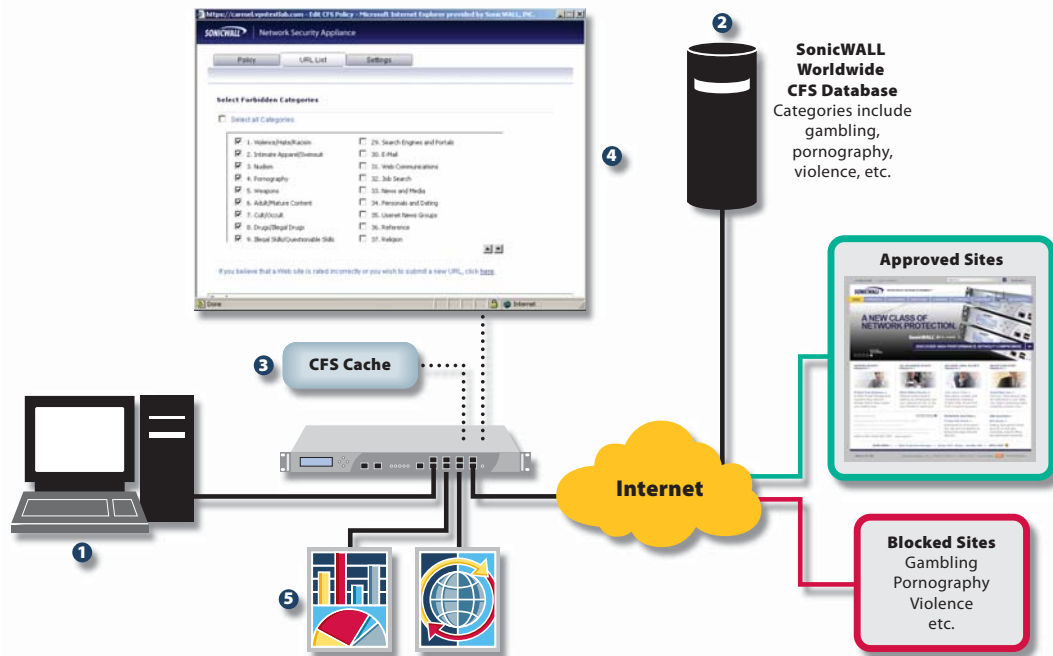
Scalable, cost-effective solution controls content filtering from the SonicWALL network security appliance, eliminating the need for additional hardware or deployment expenditures from a separate dedicated filtering server.

- Granular content filtering
- Dynamically updated rating architecture
- Regulatory reporting and compliance
- Easy-to-use Web-based management
- High-performance Web caching and rating architecture
- IP based HTTPS content filtering
- Scalable cost-effective solution

Specifications

SonicWALL Content Filtering Service Architecture

Administered through an intuitive interface, SonicWALL Content Filtering Service (CFS) enables filtering and control to take place directly over a LAN, wireless LAN or VPN. Combined with the power and scalability of SonicWALL network security appliances, and the robust reporting and management of the SonicWALL Global Management System (GMS), CFS delivers an integrated, easy-to-use, highly-manageable filtering solution for organizations of any size.



- 1 SonicWALL CFS user
- 2 Distributed SonicWALL CFS ratings data base
- 3 Local ratings cache of acceptable sites
- 4 Set URL policies to block objectionable or counter productive Web sites
- 5 Reports using SonicWALL ViewPoint or GMS

Features	CFS Premium	CFS Standard
Categories	56	12
User/Group Policies	Yes**	No
Dynamic Rating	Yes	No
Reporting	ViewPoint*	ViewPoint*
Web site caching	Yes	Yes
Safe Search Enforcement	Yes***	No
CFS Policy Enforcement per IP Range	Yes ***	No

*ViewPoint sold separately. ** SonicOS Enhanced required. ***Requires SonicOS 5.2 or greater.

Available On	CFS Premium	CFS Standard
TZ 180/180W	Yes	Yes
TZ 190/190W	Yes	Yes
TZ 100/100W	Yes	No
TZ 200/200W	Yes	No
TZ 210/210W	Yes	No
NSA Series	Yes	No
E-Class NSA Series	Yes	No

For more information on SonicWALL Content Filtering Service and our complete line of security offerings, please visit our Web site at <http://www.sonicwall.com>.

SonicWALL, Inc.

1143 Borregas Avenue
Sunnyvale CA 94089-1306

T +1 408.745.9600
F +1 408.745.9300

www.sonicwall.com

