SONICWALL

Content Filtering Service & Content Filtering Client

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.

SonicWall Content Filtering Service (CFS) running on SonicWall Unified Threat Management and next-generation firewalls (NGFWs) is a powerful protection and productivity solution that delivers unequaled content filtering enforcement for educational institutions, businesses, libraries and government agencies. Using SonicWall CFS, organizations have control over the websites students and employees can access using their IT-issued computer behind the firewall.

SonicWall CFS compares requested websites against a massive database in the cloud containing millions of rated URLs, IP addresses and websites. 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 website ratings locally on the SonicWall firewall for near-instantaneous response times.

For laptops that are used outside the firewall perimeter, the SonicWall Content Filtering Client addresses safety, security and productivity concerns by extending the controls to block harmful and unproductive web content. The client is either installed manually or automatically deployed and provisioned through a 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 websites against a highly accurate database categorizing millions of URLs, IP addresses and domains. The 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 SonicWall Capture Security Center, SonicWall Global Management System (GMS®), and SonicWall Analyzer, each of which provides real-time and historic analysis of data transmitted through the firewall, including websites 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 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 websites over encrypted HTTPS. HTTPS filtering is based on the categorical rating of websites 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 SonicWall firewall, eliminating the need for additional hardware or deployment expenditures on a separate dedicated filtering server.

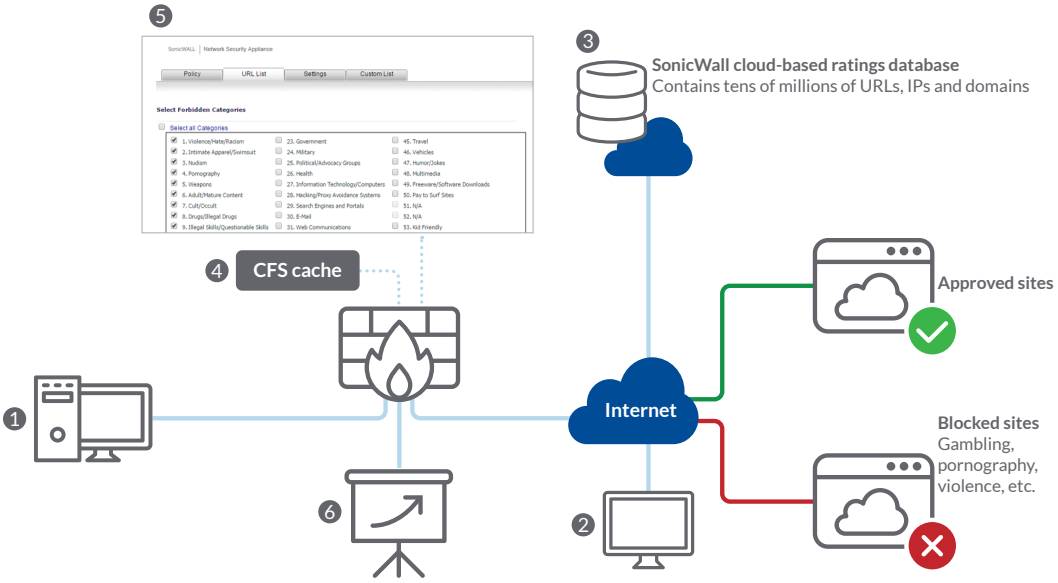
Content Filtering Client for roaming devices extends enforcement of internal web use policies to block objectionable and unproductive Internet content for devices located outside the firewall perimeter. The client enforces security and productivity policies whenever the device connects to the Internet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

SonicWall Content Filtering solutions architecture

Deployed and managed through a SonicWall firewall, 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 websites over a LAN, wireless LAN or VPN.

For roaming devices located outside the firewall perimeter, 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 SonicWall firewall and the client is managed and monitored using a powerful policy and reporting engine.

Using SonicWall Analyzer, SonicWall Capture Security Center or GMS, IT administrators can create real-time and historical reports on web usage.



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

SONICWALL CONTENT FILTERING SERVICE	
NSsp 12800 (1-year)	01-SSC-7850
NSsp 12400 (1-year)	01-SSC-7698
NSa 9650 (1-year)	01-SSC-2136
NSa 9450 (1-year)	01-SSC-1158
NSa 9250 (1-year)	01-SSC-0331
NSa 6650 (1-year)	01-SSC-8972
NSa 5650 (1-year)	01-SSC-3692
NSa 4650 (1-year)	01-SSC-3583
NSa 3650 (1-year)	01-SSC-3469
NSa 2650 (1-year)	01-SSC-1970
TZ600 Series (1-year)	01-SSC-0234
TZ500 Series (1-year)	01-SSC-0464
TZ400 Series (1-year)	01-SSC-0540
TZ350 Series (1-year)	02-SSC-1744
TZ300 Series (1-year)	01-SSC-0608
SOHO 250 Series (1-year)	02-SSC-1791
SOHO Series (1-year)	01-SSC-0676
NSv 1600 (1-year)	01-SSC-5801
NSv 800 (1-year)	01-SSC-5774
NSv 400 (1-year)	01-SSC-5690
NSv 300 (1-year)	01-SSC-5649
NSv 200 (1-year)	01-SSC-5335
NSv 100 (1-year)	01-SSC-5238
NSv 50 (1-year)	01-SSC-5203
NSv 25 (1-year)	01-SSC-5177
NSv 10 (1-year)	01-SSC-5129
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

	CONTENT FILTERING SERVICE	CONTENT FILTERING CLIENT
Categories	56+	56+
User / group policies	✓	✓
Dynamic rating	✓	✓
Reporting	Analyzer*, Capture Security Center* and GMS*	✓
Website caching	✓	✓
Safe search enforcement	✓	✓
CFS policy enforcement per IP range	✓	✓
Available on: • TZ Series • NSa Series • NSsp Series	 ✓ ✓ ✓	Endpoint devices running Windows, Chrome OS or Mac OS
YouTube Restricted Mode Support	✓	✓
HTTPS content filtering	✓	✓
Filter by schedule	✓	✓
Content filtering database	Dynamically updated base containing over 20 million URLs, IPs and domains	
Supported firmware versions/ operating systems	SonicOS 5.x and later	Firewall – Gen5: SonicOS 5.9.0.4 and later, Gen6: SonicOS 6.1.1.6 and later Laptop – Microsoft Windows 7/8/10/ Windows Server 3/ Server 8/Server 12, Chrome OS, Mac OS 10.8 and later

Analyzer, Capture Security Center and GMS are optional and sold separately.

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

For more information on SonicWall Content Filtering solutions and our complete line of security offerings, please visit our website at **www.sonicwall.com**.

About SonicWall

SonicWall has been fighting the cybercriminal industry for over 27 years defending small and medium businesses, enterprises and government agencies worldwide. Backed by research from SonicWall Capture Labs, our award- winning, real-time breach detection and prevention solutions secure more than a million networks, and their emails, applications and data, in over 215 countries and territories. These organizations run more effectively and fear less about security. For more information, visit www.sonicwall.com or follow us on Twitter, LinkedIn, Facebook and Instagram.

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Refer to our website for additional information.
www.sonicwall.com

Datasheet-ContentFilteringService-US-VG-639