

SonicWALL Content Filtering Service

PARE-FEU

Solution évolutive et dynamique de blocage des contenus Web non productifs

N'importe quel utilisateur du réseau peut, par simple navigateur, accéder facilement à des sites Internet illégaux ou inappropriés. Ces mêmes sites sont souvent infectés par des programmes malveillants qui peuvent entraîner le vol d'informations confidentielles et miner la productivité des employés. Sans compter que votre organisation peut se retrouver en situation de non-conformité, se voir refuser des financements, ou même voir sa responsabilité pénale mise en cause. Par exemple, les écoles et les bibliothèques américaines qui bénéficient du programme eRate (Education Rate) sont tenues par la loi d'installer une solution de filtrage de contenu conforme au CIPA (Children's Internet Protection Act).

SonicWALL® Content Filtering Service (CFS) assure un filtrage de contenu inégalé dans les entreprises, les établissements scolaires, les bibliothèques et les organismes publics, de même que sur des bornes Internet dispersées. Disponible sous forme d'abonnement pour tous les pare-feu SonicWALL TZ, NSA ou NSA E-Class ou au sein soit de la Comprehensive Gateway Security Suite, soit de l'offre TotalSecure, CFS bloque les contenus inappropriés, limite les risques d'engagement de la responsabilité et optimise la productivité de structures de toute taille.

SonicWALL CFS repose sur une base de données exhaustive qui réunit des millions d'URL, d'adresses IP et de sites Web. Grâce à une architecture haute performance de classification et de mise en cache, CFS actualise dynamiquement les classifications sur le pare-feu SonicWALL local afin de permettre une comparaison instantanée. Avec CFS, les administrateurs peuvent appliquer des règles d'accès ou de refus selon plus de 59 catégories d'URL, l'identité d'un individu/groupe, ou l'heure de la journée.

Caractéristiques et avantages

Filtrage granulaire des contenus. Permet à l'administrateur de bloquer ou d'appliquer la gestion de bande passante à toutes les catégories prédéfinies ou à toute combinaison de ces catégories. Les administrateurs peuvent utiliser l'authentification au niveau utilisateur (ULA) et la signature unique (SSO) pour imposer l'ouverture de session par identifiant et mot de passe. CFS bloque les contenus potentiellement nuisibles (Java,™ ActiveX,® cookies...) et peut programmer le filtrage suivant une plage horaire donnée, par exemple pendant les cours ou les heures de bureau. CFS optimise également les performances en filtrant les contenus de MI, MP3, diffusion multimédia, logiciels gratuits et autres fichiers gourmands en bande passante.

Architecture de classification à actualisation dynamique. Elle examine toutes les pages Web demandées par rapport à une base de données extrêmement précise qui répertorie des millions d'URL, d'adresses IP et de domaines. Le pare-feu SonicWALL reçoit les classifications en temps réel, qu'il compare aux règles paramétrées localement. Après quoi il autorise ou rejette la demande, en fonction des règles configurées localement par l'administrateur.

Conformité et reporting réglementaires. Ils sont assurés par l'intégration directe au Système de gestion globale primé de SonicWALL (GMS®) et au logiciel de reporting SonicWALL ViewPoint™. SonicWALL ViewPoint permet d'établir facilement des rapports graphiques détaillés ou « en un coup d'œil », à partir de données CFS en temps réel ou historiques.

Gestion Web conviviale. Assure une configuration flexible des règles et offre un contrôle total de l'usage d'Internet. Les administrateurs peuvent affecter diverses règles personnalisées à des utilisateurs individuels ou à des groupes, ainsi que définir des types de catégories. Les filtres locaux d'URL peuvent autoriser ou interdire certains domaines ou hôtes. Afin de bloquer plus efficacement tout support indésirable, les administrateurs peuvent également créer ou personnaliser les bases de filtrage.

Architecture haute performance de mise en cache Web et de classification. Permet aux administrateurs de bloquer des sites de manière simple et automatique, par catégorie. Les classifications d'URL sont mises en cache au niveau local sur le pare-feu SonicWALL, réduisant à une fraction de seconde les délais d'accès ultérieurs aux sites fréquemment consultés.

Filtrage de contenu HTTPS basé IP. Permet aux administrateurs de contrôler l'accès aux sites Web chiffrés HTTPS. Le filtrage HTTPS repose sur la classification de sites Web inappropriés en fonction de catégories de type : jeux en ligne, sites bancaires ou boursiers/trading, sites d'achat, sites de piratage ou anonymiseurs.

Solution évolutive et économique. Contrôle le filtrage de contenu depuis le pare-feu SonicWALL, ce qui évite d'avoir à ajouter du matériel ou à réaliser des dépenses supplémentaires pour installer un serveur de filtrage spécialisé.

- Filtrage granulaire des contenus
- Architecture de classification à actualisation dynamique
- Conformité et reporting réglementaires
- Gestion Web conviviale
- Architecture haute performance de mise en cache Web et de classification
- Filtrage de contenu HTTPS basé IP
- Solution évolutive et économique

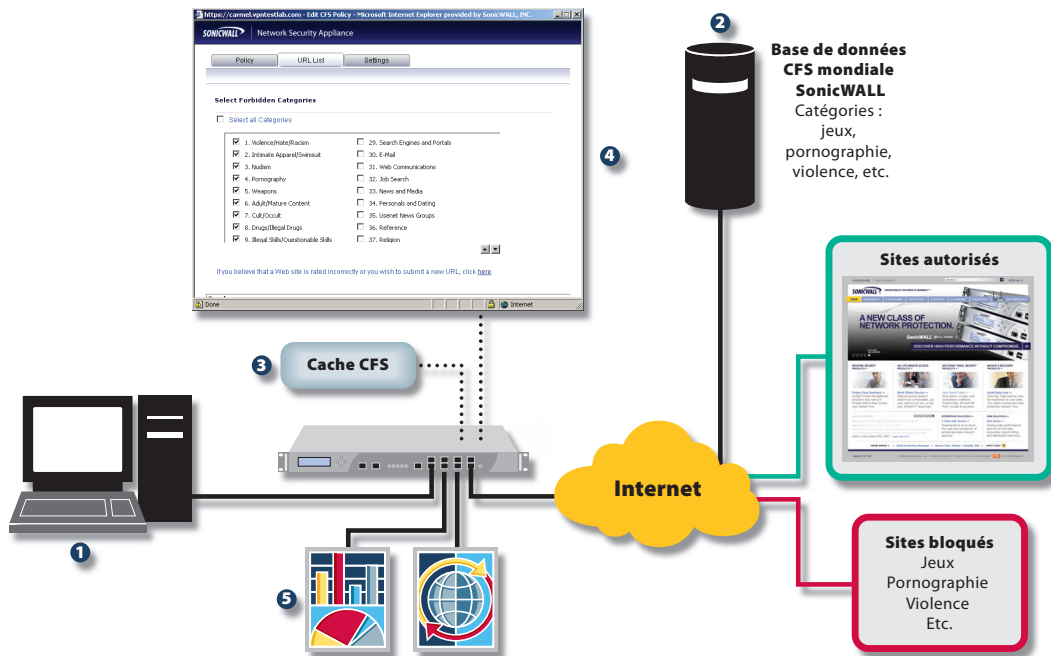
SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Spécifications

Architecture SonicWALL Content Filtering Service

Administré via une interface intuitive, SonicWALL Content Filtering Service (CFS) permet d'assurer le filtrage et le contrôle directement sur un réseau local, réseau local sans fil ou VPN. Associé aux performances et à l'évolutivité des appliances de sécurité réseau SonicWALL, ainsi qu'aux fonctions efficaces de gestion et de reporting de SonicWALL GMS, CFS constitue une solution de filtrage intégrée, conviviale et facile à gérer, idéale pour les organisations de toute taille.



- 1 Utilisateur SonicWALL CFS
- 2 Base distribuée de classifications SonicWALL CFS
- 3 Cache de classifications locales des sites acceptables
- 4 Ensemble de règles d'URL destinées à bloquer les sites Web indésirables ou contre-productifs
- 5 Rapports établis par SonicWALL ViewPoint ou GMS

Caractéristiques	CFS Premium
Catégories	59
Règles par utilisateur/groupe	Oui
Classification dynamique	Oui
Reporting	ViewPoint*
Mise en cache Web	Oui
Exécution de la recherche sécurisée	Oui
Exécution des règles CFS par plage IP	Oui

*ViewPoint vendu séparément.

Disponible sur	CFS Premium
TZ 180/180W	Oui
TZ 190/190W	Oui
TZ 100/100W	Oui
TZ 200/200W	Oui
TZ 210/210W	Oui
Série NSA	Oui
Série NSA E-Class	Oui

Pour plus d'informations sur SonicWALL Content Filtering Service et sur notre gamme de sécurité complète, consultez notre site à l'adresse suivante :

<http://www.sonicwall.com>.



SonicWALL Content Filtering Service

NSA E8500 (1 an)
01-SSC-8943

NSA E7500 (1 an)
01-SSC-7329

NSA E6500 (1 an)
01-SSC-7330

NSA E5500 (1 an)
01-SSC-7331

NSA 4500 (1 an)
01-SSC-7346

NSA 3500 (1 an)
01-SSC-7333

NSA 2400 (1 an)
01-SSC-7334

Série NSA 240 (1 an)
01-SSC-7335

Série TZ 210 (1 an)
01-SSC-7371

Série TZ 200 (1 an)
01-SSC-8634

Série TZ 100 (1 an)
01-SSC-8637

Séries TZ 180 et TZ 190 (1 an)
01-SSC-5650

Références CFS pluriannuelles disponibles.

SonicWALL France

T +33 1 49 33 73 19 France@sonicwall.com

SonicWALL BeNeLux

T +32 (0) 15 280 985 Benelux@sonicwall.com

Contacts du support SonicWALL

www.sonicwall.com/emea/4724.html

La gamme SonicWALL de solutions de sécurité dynamique



SÉCURITÉ RÉSEAU



ACCÈS DISTANT SÉCURISÉ



SÉCURISATION WEB ET DE MESSAGERIE



SAUVEGARDE ET RÉCUPÉRATION



GESTION ET RÈGLES

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™