



SonicWALL Content Filtering Service

SÉCURITÉ RÉSEAU

Solution évolutive et dynamique de blocage des contenus Web non productifs

L'Internet regorge de contenus illégaux, inappropriés et nuisibles qui peuvent pénétrer sur votre réseau par n'importe quel navigateur. Tout contenu non filtré peut transporter des programmes malveillants et freiner la productivité, 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, conformément au CIPA (Children's Internet Protection Act), d'installer une solution de filtrage de contenu.

SonicWALL® Content Filtering Service (CFS) assure un filtrage de contenu inégalé dans les entreprises, les établissements scolaires, les bibliothèques et les organismes publics, même sur des bornes Internet dispersées. 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 l'appliance de sécurité réseau SonicWALL locale afin de permettre une comparaison instantanée. Avec CFS, les administrateurs peuvent appliquer des règles d'accès ou de refus selon plus de 56 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 certaines ou toutes les catégories prédéfinies et d'appliquer les règles de manière granulaire. L'authentification au niveau utilisateur (ULA) et la signature unique (SSO) peuvent être utilisées 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. L'appliance SonicWALL reçoit les classifications en temps réel, qu'elle compare aux règles paramétrées localement. Après quoi elle 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™. Associé à ce dernier, SonicWALL CFS permet aux responsables d'établir facilement des rapports graphiques détaillés ou « en un coup d'œil », à partir de données 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 l'appliance 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 l'appliance de sécurité réseau 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

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.



SonicWALL Content Filtering Service

Premium Business Edition pour NSA E7500 (1 an)
01-SSC-7329

Premium Business Edition pour NSA E6500 (1 an)
01-SSC-7330

Premium Business Edition pour NSA E5500 (1 an)
01-SSC-7331

Premium Business Edition pour NSA E5000 (1 an)
01-SSC-7350

Premium Business Edition pour NSA 4500 (1 an)
01-SSC-7346

Premium Business Edition pour NSA 3500 (1 an)
01-SSC-7333

Premium Business Edition pour NSA 2400 (1 an)
01-SSC-7334

Premium Business Edition pour série NSA 240 (1 an)
01-SSC-7335

Premium Business Edition pour la série TZ 210 (1 an)
01-SSC-7371

Premium Business Edition pour la série TZ 200 (1 an)
01-SSC-8634

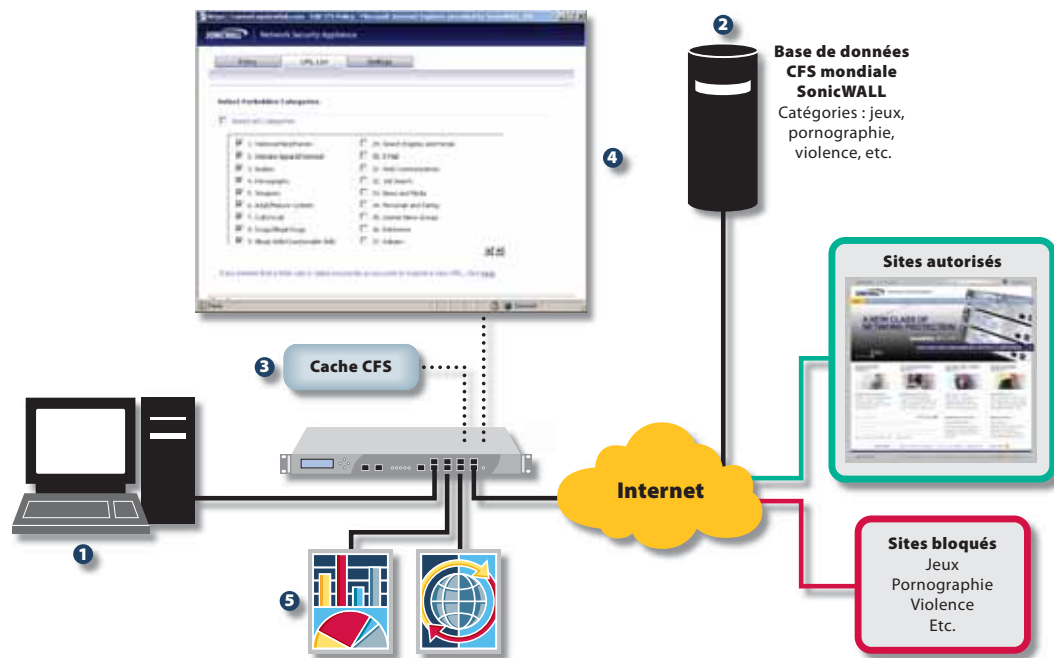
Premium Business Edition pour la série TZ 100 (1 an)
01-SSC-8637

Premium Business Edition pour les séries TZ 180 et TZ 190 (1 an)
01-SSC-5650

Standard Edition pour les séries TZ 180 et TZ 190
Nombre de nœuds illimité (1 an)
01-SSC-5505

Standard Edition pour TZ 180
10/25 nœuds (1 an)
01-SSC-7171

Références CFS pluriannuelles disponibles.



- 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	CFS Standard
Catégories	56	12
Règles par utilisateur/groupe	Oui**	Non
Classification dynamique	Oui	Non
Reporting	ViewPoint*	ViewPoint*
Mise en cache Web	Oui	Oui
Exécution de la recherche sécurisée	Oui***	Non
Exécution des règles CFS par plage IP	Oui***	Non

*ViewPoint vendu séparément. ** Requiert SonicOS Enhanced. ***Requiert SonicOS 5.2 ou version supérieure.

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

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>.

Support France

Appel gratuit : 0800.970.019
Tél. : +31 (0) 411.617.812
E-mail : sales_support-europe@sonicwall.com

Bureau France

Tél. : +33.0.1.49.33.73.09
Inside sales : +32 (0)15.293.001
E-mail : france@sonicwall.com

