Content Filtering Service et Content Filtering Client

Puissante solution de protection et de productivité pour bloquer l'accès aux contenus Web nuisibles et non productifs

Les établissements scolaires, les entreprises et les organismes publics prennent des risques importants lorsqu'ils fournissent à leurs étudiants et employés des ordinateurs gérés par le service informatique qui peuvent être utilisés pour accéder à Internet, même lorsque l'appareil est derrière le périmètre du pare-feu où les règles d'utilisation d'Internet de l'organisation sont appliquées. Ceci est particulièrement vrai lorsque ces connexions sont utilisées pour accéder à des sites contenant des informations ou des images indésirables, dangereuses, voire illégales. Ces sites peuvent être infectés par des programmes malveillants susceptibles d'être téléchargés par inadvertance et utilisés pour voler des informations confidentielles.

Il incombe notamment aux écoles de protéger leurs élèves des contenus Web inappropriés et dangereux. De plus, pour bénéficier du programme eRate (Education Rate), les écoles et les bibliothèques américaines sont tenues, conformément au CIPA (Children's Internet Protection Act), d'installer une solution de filtrage de contenu. Pour les entreprises et les organismes publics, donner aux employés un accès non contrôlé à Internet peut conduire à des pertes de productivité considérables, sans parler d'éventuels problèmes juridiques.

SonicWall Content Filtering Service (CFS) fonctionne sur la gamme UTM de SonicWall et les pare-feux de nouvelle génération. Cette puissante solution de protection et de productivité assure un filtrage de contenu hors pair pour les établissements scolaires, les entreprises, les bibliothèques ou les organismes publics. Grâce à SonicWall CFS, il est possible de contrôler derrière le pare-feu les sites Internet auxquels les étudiants et employés accèdent depuis leur ordinateur géré par le service informatique.

SonicWall CFS compare les sites Web demandés à une immense base de données Cloud contenant des millions d'URL, d'adresses IP et de sites évalués. CFS fournit aux administrateurs les outils pour créer et appliquer les règles qui autorisent ou refusent l'accès aux sites selon l'identité d'un individu/groupe ou l'heure de la journée pour plus de 56 catégories prédéfinies. De plus, CFS met en cache dynamiquement les classifications de sites Web sur le pare-feu SonicWall, ce qui permet de bénéficier de réponses quasi instantanées.

Pour les ordinateurs portables utilisés en dehors du périmètre du pare-feu, SonicWall Content Filtering Client répond aux problèmes de sécurité et de productivité en élargissant les contrôles afin de bloquer les contenus dangereux et non productifs. Ce client est automatiquement installé et configuré via le pare-feu SonicWall. En plus de fournir aux administrateurs informatiques les outils pour contrôler les accès Web pour les appareils itinérants, Content Filtering Client peut être configuré pour basculer automatiquement sur l'application des règles internes une fois que l'appareil se reconnecte au pare-feu du réseau. Le client est géré et surveillé à l'aide d'un puissant moteur de règles et de reporting dans le cloud accessible en toute transparence depuis l'interface du pare-feu. Si un client obsolète essaie de se connecter au réseau interne pour accéder à Internet, la connexion est refusée et l'utilisateur reçoit un message contenant des instructions de correction.

Caractéristiques et avantages

Le **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

Avantages :

- Protection haut de gamme
- Commandes de filtrage granulaire des contenus
- Architecture de classification à actualisation dynamique
- Analyse du trafic applicatif
- Gestion Web conviviale
- Architecture haute performance de mise en cache Web et de classification
- Filtrage de contenu HTTPS basé IP
- Solution évolutive et économique
- Content Filtering Client pour les appareils itinérants

SonicWall Content Filtering Service	
NSsp 12800 (1 an)	01-SSC-7850
NSsp 12400 (1 an)	01-SSC-7698
NSa 9650 (1 an)	01-SSC-2136
NSa 9450 (1 an)	01-SSC-1158
NSa 9250 (1 an)	01-SSC-0331
NSa 6650 (1 an)	01-SSC-8972
NSa 5650 (1 an)	01-SSC-3692
NSa 4650 (1 an)	01-SSC-3583
NSa 3650 (1 an)	01-SSC-3469
NSa 2650 (1 an)	01-SSC-1970
TZ600 Series (1 an)	01-SSC-0234
TZ500 Series (1 an)	01-SSC-0464
TZ400 Series (1 an)	01-SSC-0540
TZ300 Series (1 an)	01-SSC-0608
SOHO Series (1 an)	01-SSC-0676
NSv 1600 (1 an)	01-SSC-5801
NSv 800 (1 an)	01-SSC-5774
NSv 400 (1 an)	01-SSC-5690
NSv 300 (1 an)	01-SSC-5649
NSv 200 (1 an)	01-SSC-5335
NSv 100 (1 an)	01-SSC-5238
NSv 50 (1 an)	01-SSC-5203
NSv 25 (1 an)	01-SSC-5177
NSv 10 (1 an)	01-SSC-5129

SonicWall Content Filtering Client	
5 utilisateurs (1 an)	01-SSC-1222
10 utilisateurs (1 an)	01-SSC-1252
25 utilisateurs (1 an)	01-SSC-1225
50 utilisateurs (1 an)	01-SSC-1228
100 utilisateurs (1 an)	01-SSC-1231
250 utilisateurs (1 an)	01-SSC-1255
500 utilisateurs (1 an)	01-SSC-1237
750 utilisateurs (1 an)	01-SSC-1240
1 000 utilisateurs (1 an)	01-SSC-1243
2 000 utilisateurs (1 an)	01-SSC-1246
5 000 utilisateurs (1 an)	01-SSC-1249

de ces catégories. Les administrateurs peuvent appliquer l'authentification au niveau utilisateur (ULA) et la signature unique (SSO) pour imposer l'ouverture de session par identifiant et mot de passe. Le service CFS bloque les contenus potentiellement nuisibles (Java™, ActiveX® et cookies) et peut programmer le filtrage selon une plage horaire donnée, par exemple pendant les heures de cours ou de bureau. Il améliore également les performances en filtrant messagerie instantanée, MP3, diffusion multimédia, logiciels gratuits et autres fichiers qui mobilisent la bande passante.

Des références pluriannuelles pour Content Filtering Service et Content Filtering Client sont disponibles.

Pour plus d'informations sur les solutions de filtrage de contenu SonicWall et sur notre gamme de sécurité complète, rendez-vous sur notre site Web www.sonicwall.com.

Une **architecture de classification à actualisation dynamique** 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 et les compare aux règles paramétrées localement. Après quoi, il autorise ou rejette la demande, en fonction de la règle configurée localement par l'administrateur.

La **suite d'analyse du trafic applicatif** inclut SonicWall Capture Security Center, SonicWall Global Management System (GMS®) et SonicWall Analyzer, proposant chacun une analyse en temps réel et historique des données traversant le pare-feu, y compris les sites Web bloqués et consultés par l'utilisateur.

La 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 contrôles locaux par filtrage des URL permettent d'autoriser ou de refuser des domaines ou des hôtes spécifiques. Afin de bloquer plus efficacement tout support indésirable et non productif, les administrateurs peuvent également créer ou personnaliser les listes de filtrage.

L'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.

Le 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 en catégories de sites Web contenant des informations ou des images indésirables ou non productives : incitation à la haine et à la violence, banque et achats en ligne, etc.

La 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.

Content Filtering Client pour les appareils itinérants étend l'application des règles internes d'utilisation d'Internet afin de bloquer les contenus indésirables et non productifs pour les appareils situés en dehors du périmètre du pare-feu. Le client applique les règles de sécurité et de productivité dès que l'appareil se connecte à Internet, indépendamment de l'endroit où la connexion est établie.

Architecture de solutions de filtrage de contenu SonicWall

Déployé et géré par le biais d'un pare-feu SonicWall, SonicWall Content Filtering Service permet aux administrateurs informatiques de créer et d'appliquer les règles d'utilisation d'Internet qui empêchent les terminaux gérés situés derrière le pare-feu d'accéder à des sites Web indésirables ou non productifs sur un réseau local, un réseau local sans fil ou un VPN.

Pour les appareils itinérants situés en dehors du périmètre du pare-feu, Content Filtering Client Dell SonicWall applique les règles de sécurité et de productivité dès que l'appareil se connecte à Internet,

indépendamment de l'endroit où la connexion est établie. Le déploiement est simplifié grâce à la fonctionnalité d'exécution d'un pare-feu SonicWall et le client est géré et surveillé à l'aide d'un puissant moteur de règles et de reporting.

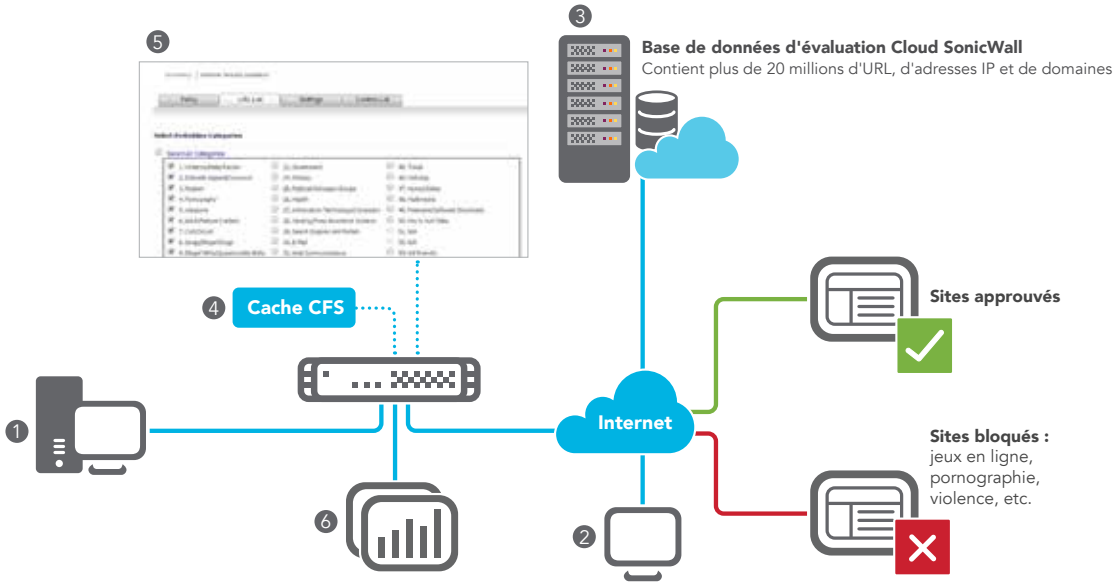
Avec SonicWall Analyzer, SonicWall Capture Security Center ou GMS, les administrateurs peuvent créer des rapports en temps réel et des rapports historiques sur l'utilisation du Web.

À propos de nous

SonicWall s'engage depuis plus de 25 ans dans la lutte contre la cybercriminalité, défendant PME et grands comptes dans le monde entier. Notre alliance de produits et de partenaires nous a permis de mettre sur pied une solution de cyberdéfense en temps réel, adaptée aux besoins spécifiques de plus de 500 000 entreprises dans plus de 150 pays, leur permettant de se concentrer sans crainte sur leur cœur de métier.

	Content Filtering Service Premium	Content Filtering Client
Catégories	Plus de 56	Plus de 56
Règles utilisateur/groupe	✓	✓
Classification dynamique	✓	✓
Création de rapports	Analyzer*, Capture Security Center* et GMS*	✓
Mise en cache de sites Web	✓	✓
Exécution de la recherche sécurisée	✓	✓
Exécution des règles CFS par plage IP	✓	✓
Disponible sur : • TZ Series • NS*a* Series • NS*sp* Series	✓ ✓ ✓	Terminaux Windows, Chrome OS ou Mac OS installés via un pare-feu SonicWall
YouTube for Schools	✓	✓
Filtrage de contenu HTTPS	✓	✓
Filtrage par horaire	✓	✓
Base de données de filtrage de contenu	Base à actualisation dynamique contenant plus de 20 millions d'URL, d'adresses IP et de domaines	
Versions de firmware/systèmes d'exploitation pris en charge	SonicOS 5.x ou plus récente	Pare-feu : 5e génération : SonicOS 5.9.0.4 et plus récente, 6e génération : SonicOS 6.1.1.6 ou plus récente Ordinateur portable : Microsoft Windows 7/8/10/ Windows Server 3/ Server 8/Server 12, Chrome OS, Mac OS 10.8 et plus récente

**Analyzer, Capture Security Center et GMS en option, vendus séparément.*



1. Utilisateur CFS SonicWall derrière le pare-feu
2. Client CF itinérant hors du périmètre du pare-feu
3. Base distribuée de classifications CFS SonicWall
4. Cache de classifications locales des sites acceptables
5. Ensemble de règles d'URL destinées à bloquer les sites Web indésirables ou contre-productifs
6. Rapports temps réel et historiques utilisant SonicWall Analyzer, Capture Security Center ou GMS

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Consultez notre site Internet pour plus d'informations.
www.sonicwall.com

Datasheet-ContentFilteringService-US-VG-MKTG2926

SONICWALL®