



FIREWALL

SonicWALL Content Filtering Service

Soluzione scalabile e dinamica per il bloccaggio di contenuti Web non produttivi

I siti Web illegali o inappropriati sono facilmente accessibili da qualsiasi utente della rete tramite un comune browser. Questi stessi siti sono spesso infestati con malware che può essere utilizzato per rubare informazioni riservate e ridurre la produttività dei dipendenti, ponendo l'azienda in condizioni di mancata conformità alle normative, con il rischio di perdere eventuali finanziamenti e persino di incorrere in responsabilità penali. Negli Stati Uniti, ad esempio, scuole e biblioteche che ricevono i cosiddetti fondi E-Rate sono obbligate per legge a installare una soluzione di filtraggio dei contenuti conforme al Children's Internet Protection Act (CIPA).

Il Content Filtering Service (CFS) di SonicWALL® è un'innovativa soluzione di filtraggio dei contenuti destinata ad aziende, istituti d'istruzione, biblioteche, enti statali e hotspot pubblici distribuiti per l'accesso a Internet. Disponibile come servizio in abbonamento per tutti i firewall delle serie TZ, NSA (Network Security Appliance) o E-Class NSA di SonicWALL o come parte integrante di un abbonamento a Comprehensive Gateway Security Suite o TotalSecure, SonicWALL CFS blocca i contenuti inappropriati, aumenta la produttività e riduce le responsabilità legali di organizzazioni di ogni dimensione.

SonicWALL CFS sfrutta un vastissimo database di milioni di URL, indirizzi IP e siti Web. Mediante un'architettura di valutazione e archiviazione in cache ad alte prestazioni, CFS aggiorna dinamicamente le valutazioni in un firewall SonicWALL locale ed effettua un confronto istantaneo. Gli amministratori possono così applicare policy di accesso o bloccaggio basate su oltre 59 categorie di URL, utenti singoli o gruppi di utenti o determinate fasce orarie.

Caratteristiche e vantaggi

Il **filtraggio granulare dei contenuti** consente agli amministratori di bloccare o applicare la gestione della larghezza di banda a tutte le categorie predefinite o ad una qualsiasi combinazione di categorie. Gli amministratori possono applicare le funzionalità di autenticazione a livello utente (ULA) e di single sign-on (SSO) per imporre l'accesso tramite nome utente e password. SonicWALL CFS è in grado di bloccare i contenuti potenzialmente dannosi come applet Java™, controlli ActiveX® e cookie e permette di pianificare il filtraggio a una qualsiasi ora del giorno, ad esempio durante le ore di lezione o l'orario di lavoro. Inoltre ottimizza le prestazioni del sistema filtrando applicazioni di messaggistica istantanea (IM) o in streaming, file MP3, freeware e altri file che potrebbero provocare un uso intenso della larghezza di banda.

L'**architettura di valutazione ad aggiornamento dinamico** confronta tutte le pagine Web richieste dagli utenti con un database in cui sono accuratamente indicizzati milioni di URL, indirizzi IP e domini. Il firewall SonicWALL riceve le valutazioni in tempo reale e le compara con le policy impostate a livello locale, quindi accetta o respinge la pagina richiesta in base a queste policy configurate localmente dall'amministratore.

Le funzioni di **reporting e conformità alle normative** sono supportate grazie all'integrazione diretta con il premiato Global Management System (GMS) e il pacchetto di reporting ViewPoint™ di SonicWALL. SonicWALL ViewPoint permette di generare con estrema semplicità report grafici immediati in tempo reale o cronologici con CFS.

L'**intuitiva gestione basata sul Web** offre flessibilità di configurazione delle policy e controllo completo sull'uso di Internet. Gli amministratori IT possono applicare policy multiple personalizzate per utenti singoli, gruppi di utenti o categorie specifiche. Il filtraggio locale degli URL può accettare o respingere determinati host e domini. Per bloccare più efficacemente il materiale inammissibile, gli amministratori possono anche creare o personalizzare i database di filtraggio.

L'**architettura di valutazione e archiviazione in cache ad alte prestazioni** permette agli amministratori di bloccare automaticamente le pagine Web in base a categorie. Le valutazioni degli URL sono archiviate localmente nella cache del firewall SonicWALL, garantendo tempi di accesso praticamente immediati per i siti più visitati.

Grazie al **filtraggio dei contenuti HTTPS basato su IP** gli amministratori possono controllare l'accesso degli utenti a siti Web attraverso HTTPS crittografati. Il filtraggio HTTPS è basato sulla valutazione di siti Web inappropriati divisi in categorie come ad es. gioco d'azzardo, banking online, brokerage e commercio online, acquisti ed hacking/proxy avoidance.

Questa **soluzione scalabile e conveniente** controlla il filtraggio dei contenuti del firewall SonicWALL, eliminando la necessità di hardware aggiuntivo o di distribuzioni da un server di filtraggio dedicato e costoso.

- **Filtraggio granulare dei contenuti**
- **Architettura di valutazione ad aggiornamento dinamico**
- **Reporting e conformità alle normative**
- **Intuitiva gestione basata sul Web**
- **Architettura di valutazione e archiviazione in cache ad alte prestazioni**
- **Filtraggio dei contenuti HTTPS basato su IP**
- **Soluzione scalabile e conveniente**

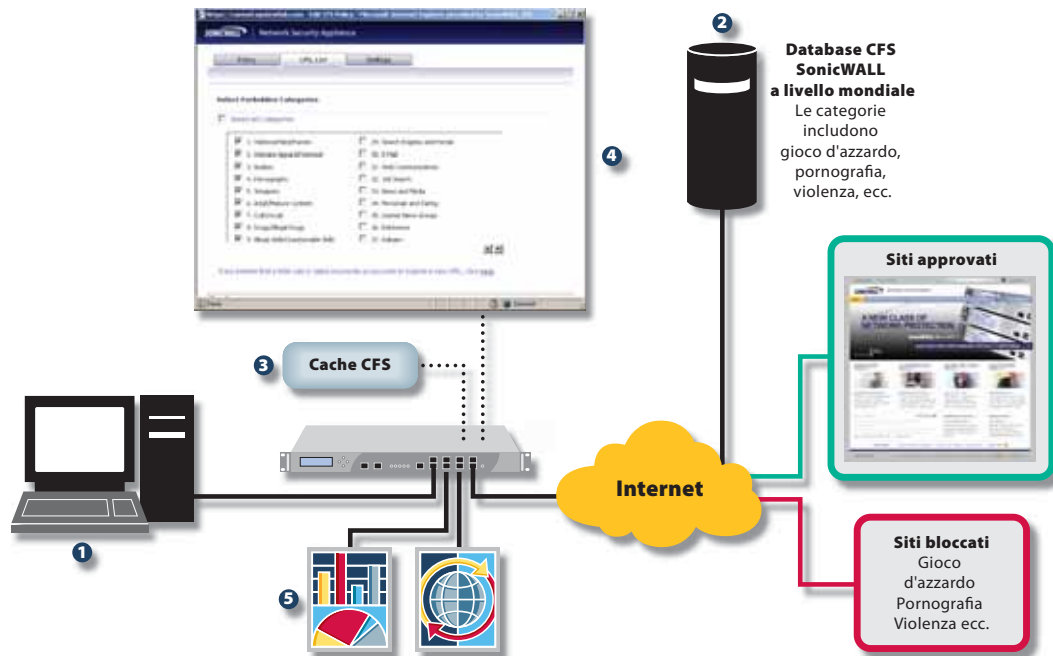
SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Specifiche tecniche

Architettura del servizio di filtraggio dei contenuti CFS di SonicWALL

Il Content Filtering Service (CFS) di SonicWALL viene gestito tramite un'interfaccia intuitiva e consente di eseguire le operazioni di filtraggio e controllo direttamente su reti LAN, wireless LAN (WLAN) o VPN. Combinato alla potenza e alla scalabilità delle appliance di sicurezza di rete SonicWALL e alle funzionalità di reporting e gestione del SonicWALL Global Management System, il Content Filtering Service (CFS) fornisce una soluzione di filtraggio integrata e semplice da utilizzare per organizzazioni di qualsiasi dimensione.



- 1 Utente SonicWALL CFS
- 2 Database di valutazione distribuito SonicWALL CFS
- 3 Cache locale valutazioni dei siti consentiti
- 4 Impostazione di policy per bloccare siti Web non idonei o improduttivi
- 5 Generazione di report tramite il SonicWALL ViewPoint o GMS

Funzionalità	CFS Premium
Categorie	59
Policy utente/gruppo	Sì
Valutazione dinamica	Sì
Reporting	ViewPoint*
Caching dei siti Web	Sì
Safe Search Enforcement	Sì
Imposizione della ricerca sicura (Safe Search Enforcement)	Sì

*ViewPoint venduto separatamente.

Disponibile con	CFS Premium
TZ 180/180W	Sì
TZ 190/190W	Sì
TZ 100/100W	Sì
TZ 200/200W	Sì
TZ 210/210W	Sì
Serie NSA	Sì
Serie E-Class NSA	Sì

Per ulteriori informazioni sul SonicWALL Content Filtering Service (CFS) e sulla nostra linea completa di servizi per la sicurezza visitate il nostro sito all'indirizzo <http://www.sonicwall.com>.

Linea di soluzioni di sicurezza dinamica SonicWALL



SICUREZZA
DI RETE



ACCESSO
REMOTO SICURO



SICUREZZA
WEB / E-MAIL



BACKUP E
RECOVERY



GESTIONE
BASATA SU POLICY

SONICWALL

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™



SonicWALL Content Filtering Service

NSA E8500 (1 anno)
01-SSC-8943

NSA E7500 (1 anno)
01-SSC-7329

NSA E6500 (1 anno)
01-SSC-7330

NSA E5500 (1 anno)
01-SSC-7331

NSA 4500 (1 anno)
01-SSC-7346

NSA 3500 (1 anno)
01-SSC-7333

NSA 2400 (1 anno)
01-SSC-7334

Serie NSA 240 (1 anno)
01-SSC-7335

Serie TZ 210 (1 anno)
01-SSC-7371

Serie TZ 200 (1 anno)
01-SSC-8634

Serie TZ 100 (1 anno)
01-SSC-8637

Serie TZ 180 e TZ 190 (1 anno)
01-SSC-5650

Sono disponibili anche abbonamenti CFS pluriennali.

SonicWALL Italy
T + 39.010.7407851

Italy@sonicwall.com

Contatti Supporto SonicWALL

www.sonicwall.com/emea/4724.html