



SonicWALL Content Filtering Service

SICUREZZA DI RETE

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

- **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**

Contenuti Web discutibili, illegali e pericolosi possono entrare nella rete attraverso il browser di qualsiasi utente. I contenuti non filtrati sono potenzialmente in grado di infettare una rete con malware, pesare sulla produttività e porre l'organizzazione 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 fondi eRate sono obbligate per legge a installare una soluzione di filtraggio dei contenuti, in conformità 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 postazioni pubbliche distribuite per l'accesso wireless a Internet. 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'appliance di sicurezza SonicWALL locale ed effettua un confronto istantaneo. Gli amministratori possono così applicare policy di accesso o bloccaggio basate su oltre 56 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 tutte le categorie predefinite, o una qualsiasi combinazione di categorie, e di applicare queste policy a livello granulare. Mediante le funzionalità di autenticazione a livello utente (ULA) e di single sign-on (SSO) è inoltre possibile 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. L'appliance 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. L'azione combinata di SonicWALL ViewPoint™ e SonicWALL CFS e di SonicWALL CFS permette di generare con estrema semplicità report grafici immediati in tempo reale o cronologici.

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 dell'appliance 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 dell'appliance di sicurezza di rete SonicWALL, eliminando la necessità di hardware aggiuntivo o di distribuzioni da un server di filtraggio dedicato e costoso.

SONICWALL®

Specifiche tecniche

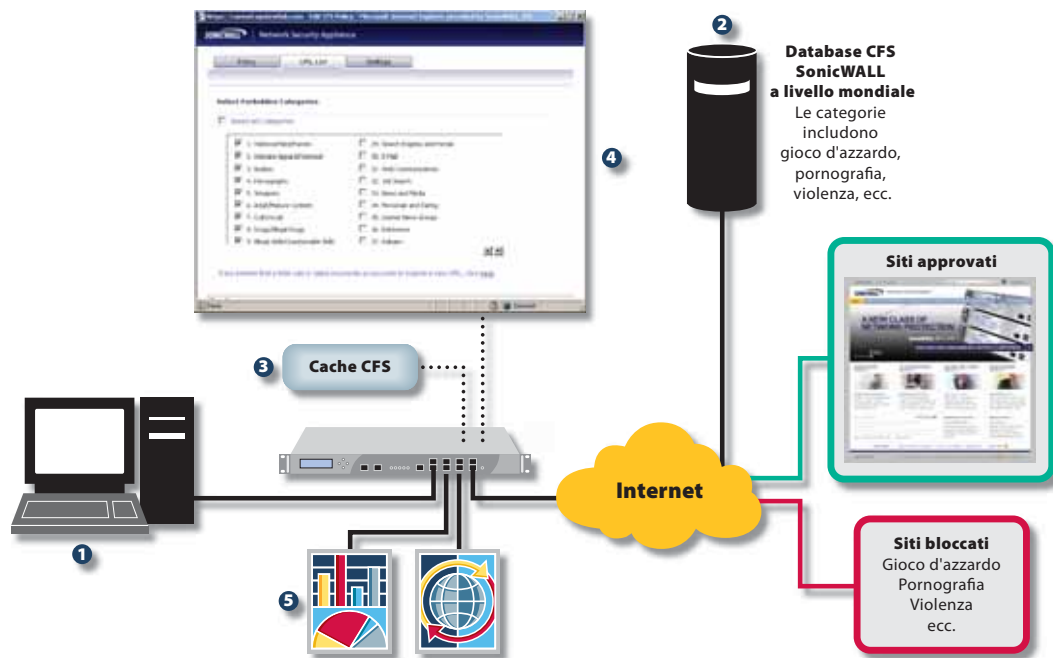
Architettura del servizio di filtraggio dei contenuti CFS di SonicWALL

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.



SonicWALL Content Filtering Service

- Edizione Premium Business per NSA E7500 (1 anno)
01-SSC-7329
 - Edizione Premium Business per NSA E6500 (1 anno)
01-SSC-7330
 - Edizione Premium Business per NSA E5500 (1 anno)
01-SSC-7331
 - Edizione Premium Business per NSA 5000 (1 anno)
01-SSC-7350
 - Edizione Premium Business per NSA 4500 (1 anno)
01-SSC-7346
 - Edizione Premium Business per NSA 3500 (1 anno)
01-SSC-7333
 - Edizione Premium Business per NSA 2400 (1 anno)
01-SSC-7334
 - Edizione Premium Business per la serie NSA 240 (1 anno)
01-SSC-7335
 - Edizione Premium Business per la serie TZ 210 (1 anno)
01-SSC-7371
 - Edizione Premium Business per la serie TZ 200 (1 anno)
01-SSC-8634
 - Edizione Premium Business per la serie TZ 100 (1 anno)
01-SSC-8637
 - Edizione Premium Business per le serie TZ 180 e TZ 190 (1 anno)
01-SSC-5650
 - Edizione Standard per le serie TZ 180 e TZ 190
Nodi illimitati (1 anno)
01-SSC-5505
 - Edizione Standard per TZ 180, 10/25 nodi (1 anno)
01-SSC-7171
- Sono disponibili anche abbonamenti CFS pluriennali.



- 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	CFS Standard
Categorie	56	12
Policy utente/gruppo	SI**	No
Valutazione dinamica	SI	No
Reporting	ViewPoint*	ViewPoint*
Caching dei siti Web	SI	SI
Imposizione della ricerca sicura (Safe Search Enforcement)	SI***	No
Applicazione di policy CFS in base ai range di IP	SI***	No

*ViewPoint venduto separatamente. **Richiede SonicOS Enhanced. ***Richiede SonicOS 5.2 o superiore.

Disponibile con	CFS Premium	CFS Standard
TZ 180/180W	SI	SI
TZ 190/190W	SI	SI
TZ 100/100W	SI	No
TZ 200/200W	SI	No
TZ 210/210W	SI	No
Serie NSA	SI	No
Serie E-Class NSA	SI	No

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>.

Italia / Supporto

Numero verde: 800.909.106
Telefono: +31 (0) 411.617.814
E-mail: sales_support-europe@sonicwall.com

Italia / Uffici

Telefono: +39.010.7407851
E-mail: italy@sonicwall.com

