Content Filtering Service e Content Filtering Client

Potente soluzione per protezione e produttività per bloccare l'accesso ai contenuti Web pericolosi e improduttivi

Gli istituti di istruzione, le imprese e gli enti governativi si assumono rischi notevoli quando forniscono agli studenti e ai dipendenti computer messi a disposizione dai reparti informatici e che possono essere utilizzati per accedere a Internet, anche quando il dispositivo si trova all'interno del perimetro del firewall, dove vengono applicate le policy organizzative di utilizzo del Web. Ciò è particolarmente vero quando tali connessioni vengono utilizzate per accedere a siti che contengono informazioni e immagini inappropriate, pericolose o addirittura illegali. Questi siti potrebbero inoltre essere stati infettati da malware che può essere scaricato inavvertitamente e quindi utilizzato per rubare informazioni riservate.

Le scuole, in particolare, hanno la responsabilità di proteggere gli studenti da contenuti sul Web inappropriati e pericolosi. Inoltre, per ricevere i fondi, ad esempio gli eRate negli Stati Uniti, sia le scuole sia le biblioteche hanno l'obbligo di legge di installare una soluzione di filtraggio dei contenuti che sia conforme a leggi come il Children's Internet Protection Act (CIPA). Per le aziende e gli enti pubblici, fornire ai dipendenti un accesso Web non controllato può risultare in una navigazione Web improduttiva e creare enormi perdite di produttività, senza parlare della potenziale responsabilità legale.

SonicWall Content Filtering Service (CFS) gira su SonicWall Unified Threat Management e firewall di nuova generazione (NGFW) ed è una potente soluzione di protezione e produttività in grado di implementare un filtraggio dei contenuti senza eguali per istituti di istruzione, biblioteche ed enti pubblici. Utilizzando SonicWall CFS, le aziende possono tenere sotto controllo i siti Web visitati da studenti e dipendenti attraverso i computer messi a loro disposizione dal reparto informatico quando si trovano all'interno del firewall.

SonicWall CFS confronta i siti Web richiesti con un enorme database sul cloud contenente milioni di valutazioni di URL, indirizzi IP e siti Web. CFS fornisce agli amministratori gli strumenti per creare e applicare policy che consentono o negano l'accesso a siti sulla base di identità individuali o di gruppo oppure in base all'ora del giorno, per oltre 56 categorie predefinite. CFS memorizza inoltre dinamicamente le valutazioni dei siti nella cache locale su firewall SonicWall per ottenere tempi di risposta quasi immediati.

Per i laptop che vengono utilizzati al di fuori del perimetro del firewall, il SonicWall Content Filtering Client affronta le questioni di sicurezza, protezione e produttività estendendo i controlli al fine di bloccare i contenuti Web pericolosi e improduttivi. Il client viene implementato automaticamente e fornito attraverso un firewall SonicWall. Oltre a fornire agli amministratori IT gli strumenti per controllare l'accesso basato sul Web di dispositivi circolanti, il Content Filtering Client può essere configurato per passare automaticamente all'implementazione della policy interna nel momento in cui il dispositivo si ricollega al firewall di rete. Il client è gestito e monitorato utilizzando un potente motore per policy e rapporti sul cloud, al quale si accede in modo trasparente attraverso l'interfaccia del firewall. Nel caso in cui un client non aggiornato tenti di connettersi alla rete interna per accedere a Internet, la connessione viene rifiutata e l'utente riceve un messaggio con istruzioni sulle procedure di risoluzione.

Vantaggi:

- Protezione avanzata
- Controlli per filtraggio granulare dei contenuti
- Architettura di valutazione ad aggiornamento dinamico
- Analisi del traffico delle applicazioni
- 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
- Content Filtering Client per dispositivi in roaming

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

SonicWall Content Filtering Client	
5 utenti (1 anno)	01-SSC-1222
10 utenti (1 anno)	01-SSC-1252
25 utenti (1 anno)	01-SSC-1225
50 utenti (1 anno)	01-SSC-1228
100 utenti (1 anno)	01-SSC-1231
250 utenti (1 anno)	01-SSC-1255
500 utenti (1 anno)	01-SSC-1237
750 utenti (1 anno)	01-SSC-1240
1.000 utenti (1 anno)	01-SSC-1243
2.000 utenti (1 anno)	01-SSC-1246
5.000 utenti (1 anno)	01-SSC-1249

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. CFS è in grado di bloccare contenuti potenzialmente dannosi come applet Java™, controlli ActiveX® e cookies, e permette di pianificare il filtraggio in base all'ora del giorno, ad esempio durante l'orario scolastico o lavorativo. 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.

Sono disponibili SKU pluriennali per Content Filtering Service e Content Filtering Client.

Per ulteriori informazioni sulle soluzioni SonicWall Content Filtering (CFS) e sulla nostra linea completa di servizi per la sicurezza visitate il nostro sito all'indirizzo www.sonicwall.com.

Un'**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 compara ciascuna di esse con le policy impostate a livello locale, quindi accetta o respinge la pagina richiesta in base a queste policy configurate localmente dall'amministratore.

La **suite di analisi del traffico delle applicazioni** include SonicWall Capture Security Center, SonicWall Global Management System (GMS®) e SonicWallAnalyzer, ciascuno dei quali fornisce analisi storica e in tempo reale dei dati trasmessi attraverso il firewall, inclusi i siti Web bloccati e visitati per utente.

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 non appropriato e non produttivo, gli amministratori possono anche creare o personalizzare gli elenchi di filtraggio.

L'**architettura di valutazione e archiviazione in cache Web ad alte prestazioni** permette agli amministratori di bloccare automaticamente i siti 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 contenenti informazioni e immagini non idonee o non produttive e divisi in categorie come ad es. contenuti violenti, di istigazione all'odio, banking e commercio online, e altre.

Questa **soluzione scalabile e conveniente** controlla il filtraggio dei contenuti direttamente dal firewall SonicWall, eliminando la necessità di hardware aggiuntivo o di costose installazioni su un server di filtraggio dedicato.

Il **Content Filtering Client per dispositivi in roaming** estende l'applicazione delle policy interne sull'utilizzo del Web per bloccare i contenuti Internet non idonei e improduttivi anche sui dispositivi che si trovano al di fuori del perimetro del firewall. Il client implementa policy di sicurezza e produttività ogni volta che il dispositivo si connette a Internet a prescindere dal luogo in cui viene stabilita la connessione.

Architettura delle soluzioni SoniWall Content Filtering

Implementato e gestito attraverso un firewall SonicWall, il SonicWall Content Filtering Service consente agli amministratori IT di creare e attuare policy di utilizzo di Internet in grado di bloccare i dispositivi endpoint rilasciati dal reparto IT, posti dietro il firewall, evitando che possano accedere a siti Web inappropriati e non produttivi attraverso una rete LAN, wireless LAN o VPN.

Per i dispositivi in roaming al di fuori del perimetro del firewall, SonicWall Content Filtering Client estende le policy di sicurezza e produttività ogni volta che il dispositivo si connette a Internet indipendentemente da dove viene stabilita la connessione. L'implementazione è semplificata dall'utilizzo della funzionalità di messa in pratica di un firewall SonicWall e il client viene gestito e monitorato utilizzando un potente motore di policy e reporting.

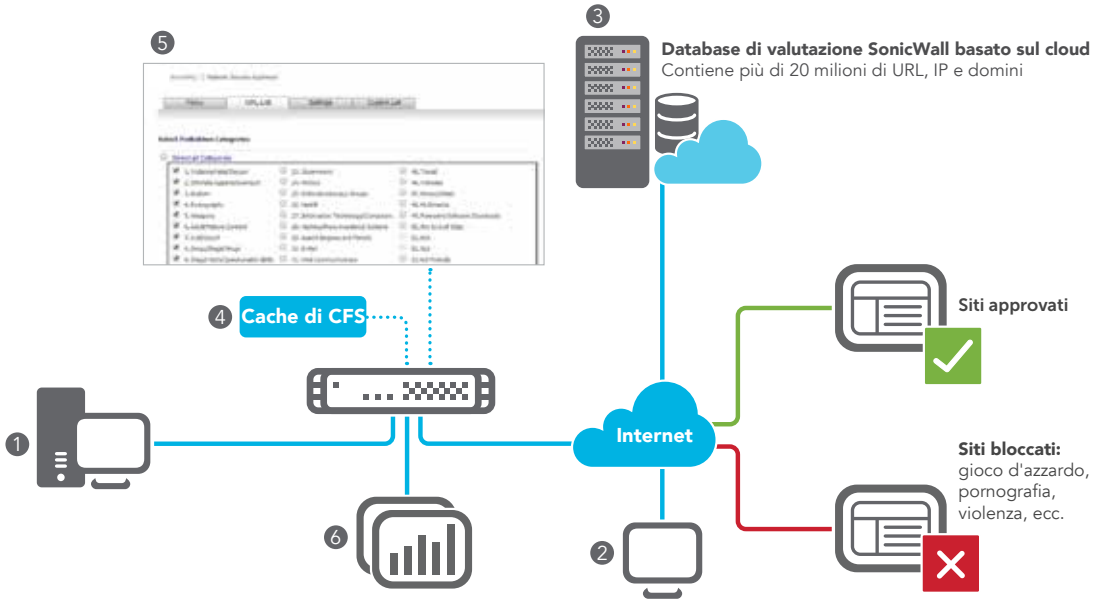
Usando SonicWall Analyzer, SonicWall Capture Security Center o GMS, gli amministratori IT possono creare rapporti storici e in tempo reale sull'utilizzo del Web.

Informazioni su SonicWall

Da oltre 25 anni SonicWall combatte il crimine informatico, proteggendo piccole, medie e grandi imprese in ogni parte del mondo. La nostra combinazione di prodotti e partner ha permesso di realizzare una soluzione di difesa informatica in tempo reale ottimizzata per le specifiche esigenze di oltre 500.000 aziende in più di 150 paesi, per consentire loro di fare più affari con maggior sicurezza.

	Content Filtering Service Premium	Content Filtering Client
Categorie	56+	56+
Policy utente/gruppo	✓	✓
Valutazione dinamica	✓	✓
Creazione di rapporti	Analyzer*, Capture Security Center* e GMS*	✓
Caching di siti Web	✓	✓
Safe Search Enforcement	✓	✓
Applicazione di policy CFS in base ai range di IP	✓	✓
Disponibile con: • Serie TZ • Serie NS*a* • Serie NS*sp*	✓ ✓ ✓	Dispositivi end point con Windows, Chrome OS oppure Mac OS implementati tramite un firewall SonicWall
YouTube for Schools	✓	✓
Filtraggio dei contenuti HTTPS	✓	✓
Filtro per pianificazione	✓	✓
Database di filtraggio dei contenuti	Base aggiornata dinamicamente contenente oltre 20 milioni di URL, IPS e domini	
Versioni firmware / Sistemi operativi supportati	SonicOS 5.x e successivi	Firewall – Gen5: SonicOS 5.9.0.4 e successivi, Gen6: SonicOS 6.1.1.6 e successivi; Laptop – Microsoft Windows 7/8/10/ Windows Server 3/ Server 8/Server 12, Chrome OS, Mac OS 10.8 e successivi

**Analyzer, Capture Security Center e GMS sono opzionali e venduti separatamente*



1. Utente SonicWall CFS dietro il firewall
2. Utente client CF mobile al di fuori del perimetro del firewall
3. Database distribuito di valutazione SonicWall CFS
4. Cache locale valutazioni dei siti consentiti
5. Impostazione di policy URL per bloccare siti Web non idonei o improduttivi
6. Rapporti in tempo reale e storici utilizzando SonicWall Analyzer, Capture Security Center o GMS

SonicWall, Inc.
1033 McCarthy Boulevard | Milpitas, CA 95035
Per maggiori informazioni consultare il nostro sito web.
www.sonicwall.com

Datasheet-ContentFilteringService-US-VG-MKTG2926

SONICWALL®