



SonicWALL Comprehensive Anti-Spam Service

GESTIONE UNIFICATA DELLE MINACCE

Protezione anti-spam immediata al gateway

- **Gestione avanzata della reputazione (ARM)**
- **Gestione avanzata dei contenuti (ACM) basata su cloud**
- **Routing flessibile delle e-mail indesiderate**
- **Opzione Posta indesiderata**
- **GRID Anti-Virus**
- **Elenchi di blocco e autorizzazione integrati**
- **Reporting e logging**
- **Integrazione LDAP flessibile**
- **Supporto di sistemi di sicurezza e-mail downstream**

Quasi il 94% della posta elettronica classificata come indesiderata è costituito da spam, tentativi di phishing ed e-mail con virus allegati che non solo distolgono l'attenzione degli utenti dalle attività lavorative, con conseguenze sulla produttività, ma possono compromettere l'efficacia dell'intera rete di comunicazioni. La rimozione della posta indesiderata a livello del gateway ottimizza l'efficienza della rete e migliora la produttività dei dipendenti e della posta elettronica.

SonicWALL® Comprehensive Anti-Spam Service (CASS) offre a piccole e medie imprese una protezione completa da spam e virus, con possibilità d'implementazione immediata sui firewall SonicWALL esistenti. CASS velocizza i tempi di distribuzione, semplifica l'amministrazione e riduce l'impegno degli amministratori grazie al consolidamento delle soluzioni, fornendo servizi anti-spam attivabili con un solo clic del mouse e configurabili in soli 10 minuti. CASS offre completa protezione anti-spam, anti-phishing e anti-malware, verifica della reputazione degli IP tramite la rete GRID (Global Response Intelligent Defense) di SonicWALL, gestione avanzata dei contenuti, prevenzione da attacchi DoS (Denial of Service), quarantena completa e riepiloghi della posta indesiderata personalizzabili per ogni utente. Grazie a prestazioni di filtraggio superiori a quelle previste dalle liste RBL, CASS offre un'efficacia anti-spam superiore al 98%, bloccando più dell'80% dello spam a livello del gateway. Per il controllo dei restanti messaggi e-mail utilizza avanzate tecniche anti-spam quali il filtraggio Adversarial Bayesian™.

Caratteristiche e vantaggi

La **gestione avanzata della reputazione (ARM)** utilizza la reputazione IP del mittente per respingere messaggi di spam, phishing e virus allegati a livello di connessione, prima che possano penetrare nella rete. Le informazioni in tempo reale sulla reputazione del mittente, provenienti dalla rete SonicWALL GRID, consentono di identificare e bloccare i messaggi provenienti da spammer conosciuti. Questo servizio elimina la necessità dei servizi black list in tempo reale meno efficaci, più lenti e soggetti ad errori.

La **gestione avanzata dei contenuti (ACM) basata su cloud** elimina le rimanenti e-mail indesiderate utilizzando le collaudate tecniche anti-spam di SonicWALL, tra cui analisi bayesiana avversariale, dati della rete GRID, motore di analisi inferenziale delle immagini, rilevazione di sequenze di caratteri senza senso e filtri bayesiani anti-phishing. L'architettura cloud based utilizza queste tecniche anti-spam avanzate senza rallentare le prestazioni del firewall e la velocità della rete.

Il **routing flessibile delle e-mail indesiderate** classifica i messaggi spazzatura come spam, probabile spam, phishing, probabile phishing, virus e probabile virus. I messaggi di ogni categoria possono essere rifiutati, contrassegnati e consegnati, inviati alla cartella Posta indesiderata dell'utente oppure eliminati, per garantire il controllo completo e la conformità ai requisiti aziendali e di legge.

L'opzione **Posta indesiderata** consente agli utenti di configurare velocemente caselle per l'archiviazione di questo tipo di messaggi. Gli utenti possono ricevere e-mail di riepilogo del contenuto della casella, utilizzabili per visualizzare i messaggi (come testo) e, se opportuno, rimuoverli dalla posta indesiderata. Il reparto IT mantiene il controllo su categorie da visualizzare e piani di conservazione ed eliminazione dei riepiloghi della posta indesiderata.

SonicWALL GRID Anti-Virus viene attivato automaticamente insieme al servizio SonicWALL CASS per rilevare le e-mail infette basate su SMTP e reinstrarle secondo le modalità definite dall'amministratore (ad esempio rifiutate o eliminate) a livello del gateway. Se acquistati separatamente, i servizi SonicWALL Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention e SonicWALL Enforced Client Anti-Virus and Anti-Spyware offrono protezione completa contro i virus su tutti i livelli.

Gli **elenchi di blocco e autorizzazione integrati** nelle appliance di sicurezza SonicWALL consentono di bloccare o autorizzare gli indirizzi IP a livello del gateway, con possibilità di attivare un controllo granulare tramite elenchi di blocco/autorizzazione basati su utenti, aziende o livelli di elenchi. Questa funzionalità è completamente supportata dal servizio CASS e non richiede configurazioni aggiuntive o addestramenti particolari.

Le funzionalità di **reporting e logging** integrate nelle appliance SonicWALL permettono di visualizzare, con un semplice clic, stato dei servizi, statistiche e voci del file di log corrispondenti ai nomi dei servizi. Lo stato dei servizi mostra la disponibilità del Comprehensive Anti-Spam Service, delle caselle di posta indesiderata e del server di posta downstream.

L'**integrazione LDAP** flessibile consente una gestione potente, facile e sicura degli utenti e offre maggiore flessibilità grazie al supporto per l'integrazione di più LDAP.

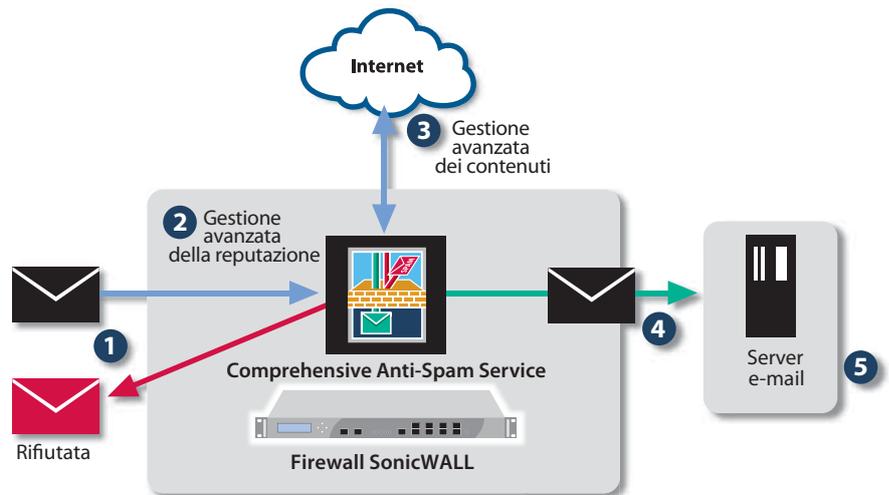
Supporto di sistemi di sicurezza e-mail downstream quali policy di conformità o di corporate governance, policy e preferenze per utente, reporting avanzato e altro ancora, secondo necessità.

SONICWALL®

DYNAMIC SECURITY FOR THE GLOBAL NETWORK™

Specifiche tecniche

Come funziona il SonicWALL Comprehensive Anti-Spam Service



- 1 Il traffico SMTP arriva al firewall SonicWALL
- 2 Il Comprehensive Anti-Spam Service controlla in tempo reale la reputazione dell'IP del server di invio mediante la gestione avanzata della reputazione (ARM), che riceve informazioni in tempo reale da oltre 4 milioni di terminali in tutto il mondo per poter determinare la reputazione dei server che inoltrano le e-mail. Fino all'80% della posta indesiderata può essere respinta a livello di connessione, riducendo sensibilmente il carico di lavoro del firewall.
- 3 Il traffico e-mail rimanente viene elaborato dal servizio di gestione avanzata dei contenuti (ACM) basato su cloud, che utilizza le collaudate tecniche di rilevamento dello spam di SonicWALL.
- 4 I messaggi sicuri vengono consegnati al server e-mail.
- 5 In alternativa, la posta indesiderata può essere consegnata alle caselle di posta indesiderata di SonicWALL sul server e-mail e ogni utente può ricevere messaggi e-mail con un riepilogo della posta indesiderata eliminata.

A chi è destinato il SonicWALL Comprehensive Anti-Spam Service

Le aziende più piccole possono sfruttare il loro investimento in un firewall SonicWALL per avere la certezza che, tramite il servizio CASS, al proprio server di posta vengano inoltrati solo messaggi e-mail sicuri. Gli amministratori possono gestire il servizio CASS mediante un'unica interfaccia integrata sul firewall. Le grandi aziende possono stratificare la propria protezione anti-spam installando il servizio CASS a monte di una soluzione di protezione e-mail di SonicWALL per bloccare oltre l'80% della posta indesiderata a livello di connessione, riducendo così il carico di lavoro dell'infrastruttura a valle. Le aziende distribuite, che ricevono la posta in più sedi, possono implementare CASS su firewall SonicWALL remoti per ridurre il traffico di rete legato allo spamming e utilizzare SonicWALL Email Security per centralizzare i servizi di protezione della posta elettronica.

Piattaforme e server e-mail supportati

SonicWALL Comprehensive Anti-Spam Service è disponibile come servizio in abbonamento con i seguenti prodotti SonicWALL:

- Serie TZ 100, TZ 200 e TZ 210 con SonicOS 5.6.3 o successivo installato
- Tutte le appliance delle serie SonicWALL NSA e SonicWALL E-Class NSA con SonicOS 5.6.3 o successivo installato
- Le piattaforme e/o le versioni SonicOS non elencate non sono supportate

SonicWALL Comprehensive Anti-Spam Service funziona con qualsiasi server e-mail che accetta la posta in entrata SMTP.

Opzioni incluse nel Comprehensive Anti-Spam Service

L'opzione **Posta indesiderata** richiede l'installazione dell'applicazione Junk Store (fornita come parte del servizio) su un server (generalmente il server e-mail del cliente) dotato di Windows Server 2003 o Windows Server 2008.



Comprehensive Anti-Spam Service

Comprehensive Anti-Spam Service per la serie TZ 100 (1 anno)
01-SSC-8985

Comprehensive Anti-Spam Service per la serie TZ 200 (1 anno)
01-SSC-8988

Comprehensive Anti-Spam Service per la serie TZ 210 (1 anno)
01-SSC-8991

Comprehensive Anti-Spam Service per NSA 240 (1 anno)
01-SSC-8994

Comprehensive Anti-Spam Service per NSA 2400 (1 anno)
01-SSC-8997

Comprehensive Anti-Spam Service per NSA 3500 (1 anno)
01-SSC-9000

Sono anche disponibili abbonamenti pluriennali. Visitare www.sonicwall.com.

Comprehensive Anti-Spam Service supporta un numero illimitato di utenti, ma è consigliato per 250 o meno utenti.

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 Italy
T + 39.010.7407851
Italy@sonicwall.com
Contatti Supporto SonicWALL
www.sonicwall.com/emea/4724.html