Comprehensive Anti-Spam Service

Protezione anti-spam immediata al gateway

Quasi l'80% 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 comunicazione aziendale. 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'installazione immediata sui firewall SonicWall esistenti. Il servizio CASS velocizza i tempi di distribuzione, semplifica la gestione e riduce l'impegno degli amministratori grazie al consolidamento delle soluzioni, fornendo servizi anti-spam attivabili con un semplice clic del mouse e configurabili in soli 10 minuti. CASS offre protezione completa contro spam, phishing e malware in ingresso, verifica della reputazione degli IP tramite la rete SonicWall Capture Threat, gestione avanzata dei contenuti, prevenzione da attacchi Denial of Service (DoS), quarantena completa e riepiloghi della posta indesiderata personalizzabili per ogni utente. Grazie a prestazioni di filtraggio superiori a quelle previste dalle liste RBL, il servizio CASS offre un'efficacia antispam superiore al 99%, bloccando più dell'80% dello spam a livello del gateway grazie a tecniche di rilevamento avanzate come il filtraggio Adversarial Bayesian™ e filtri basati sull'apprendimento automatico.

Caratteristiche e vantaggi

Blocco degli attacchi di spam, phishing e virus mediante comprovate tecniche brevettate*, tra cui i controlli della reputazione che non solo verificano l'attendibilità del mittente in base all'indirizzo IP, ma anche quella dei contenuti, della struttura, dei collegamenti, delle immagini e degli allegati. Per individuare le nuove minacce e quelle già note in agguato, i contenuti delle e-mail vengono analizzati con tecnologie avanzate come il filtraggio bayesiano, l'analisi delle immagini e il rilevamento di contenuti sospetti. L'architettura basata su cloud utilizza queste tecniche antispam avanzate senza rallentare le prestazioni del firewall e la velocità della rete.

Informazioni sulle minacce in tempo reale tramite SonicWall Capture Threat Network, che raccoglie e analizza informazioni da elenchi di minacce del settore e sottopone milioni di e-mail a rigorosi test e valutazioni ogni giorno, assegnando poi un punteggio alla reputazione di mittenti e contenuti per identificare le nuove minacce in tempo reale e fornire una protezione mirata e aggiornata contro i nuovi attacchi di spam, con in più la garanzia di recapitare solo e-mail legittime.

SonicWall Capture Cloud utilizza la tecnologia SonicWall Capture Threat Network per fornire un'efficace protezione contro virus e spyware basata sul cloud.

Il **routing flessibile delle e-mail indesiderate** classifica i messaggi di posta indesiderata 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

Vantaggi:

- Blocco degli attacchi di spam
- Aggiornamento delle informazioni sulle minacce in tempo reale tramite SonicWall Capture Threat Network
- Capture Cloud
- Opzione Posta indesiderata
- Elenchi di blocco e autorizzazione integrati
- Reportistica e log integrati
- Integrazione LDAP
- Supporto di sistemi di sicurezza e-mail a valle

*Brevetti statunitensi: 7,814,545; 7,343,624; 7,665,140; 7,653,698; 7,546,348

messaggi. Gli utenti possono ricevere e-mail con un 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 sulle categorie da visualizzare e sulla pianificazione ed eliminazione dei riepiloghi della posta indesiderata.

Gli **elenchi di blocco e autorizzazione integrati** nelle appliance di sicurezza SonicWall consentono di bloccare o autorizzare gli indirizzi IP a livello del gateway. Gli amministratori possono applicare un controllo granulare tramite elenchi di blocco/autorizzazione a livello di utente, azienda o elenco. Questa funzionalità è pienamente supportata dal servizio CASS e non richiede configurazioni o apprendimento aggiuntivi.

Le **funzionalità di reportistica e log integrate** nei firewall SonicWall permettono di visualizzare con un semplice clic lo stato dei servizi, le statistiche e le voci del file di log in base al nome dei servizi. Lo stato dei servizi mostra la disponibilità del servizio CASS, delle caselle di posta indesiderata e del server e-mail downstream.

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

Supporto di sistemi di sicurezza e-mail downstream quali policy di conformità o di governance aziendale, policy e preferenze per singolo utente, creazione di rapporti avanzati e altro ancora, secondo necessità.

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, vengano inoltrati solo messaggi e-mail attendibili e sicuri al proprio server di posta. Gli amministratori possono gestire il servizio CASS mediante un'unica interfaccia integrata nel firewall. Le grandi aziende possono stratificare la propria protezione antispam installando il servizio CASS a monte di una soluzione SonicWall Email Security 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 installare CASS su firewall SonicWall remoti per ridurre il traffico di rete associato allo spam 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:

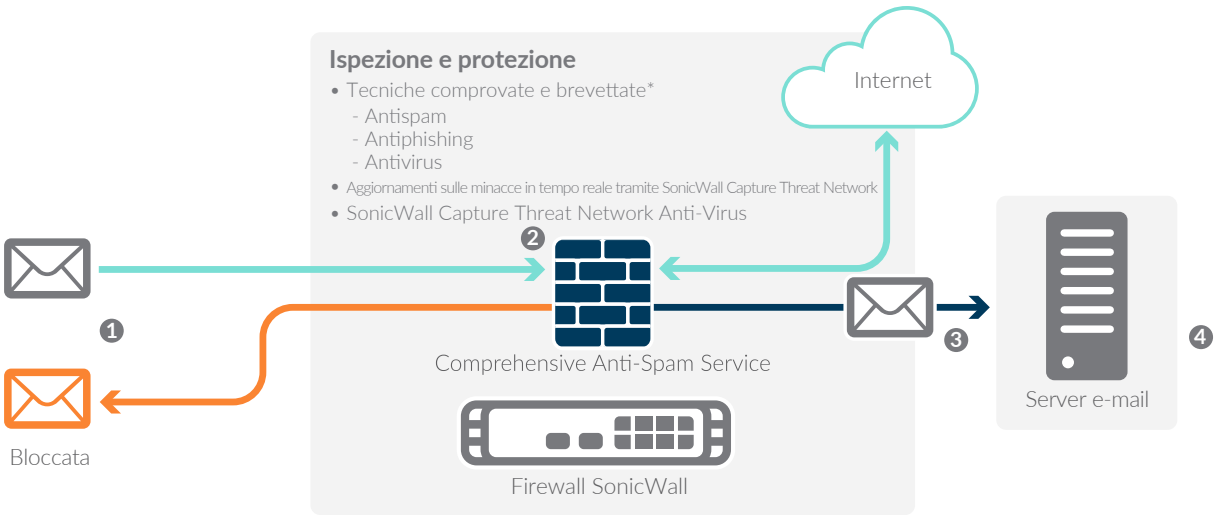
- Tutti i firewall delle serie SonicWall TZ e Network Security appliance (NS*a*)* con SonicOS 5.6.3 o superiore installato
- Le piattaforme e/o le versioni SonicOS non elencate non sono supportate

SonicWall Comprehensive Anti-Spam Service funziona con qualsiasi server e-mail che accetti messaggi SMTP in entrata.

Opzioni incluse in 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 2008 o Windows Server 2012.

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. SonicWall Capture Threat Network riceve informazioni in tempo reale da oltre 4 milioni di terminali in tutto il mondo per determinare l'attendibilità dei server che inoltrano le e-mail. Fino all'80% della posta indesiderata può essere bloccato a livello di connessione, riducendo sensibilmente il carico di elaborazione del firewall. Il traffico e-mail rimanente viene analizzato dal SonicWall Capture Threat Network basato su cloud, che utilizza le collaudate tecniche di rilevamento dello spam di SonicWall.

3 I messaggi di posta elettronica legittimi vengono consegnati al server e-mail.

4 In alternativa, la posta indesiderata può essere consegnata alle caselle di posta indesiderata di SonicWall sul server e-mail e ogni utente può ricevere e-mail con un riepilogo della posta indesiderata eliminata.

Comprehensive Anti-Spam Service

01-SSC-0682 Serie SOHO (1 anno)

01-SSC-0632 Serie TZ300 (1 anno)

01-SSC-0561 Serie TZ400 (1 anno)

01-SSC-0482 Serie TZ500 (1 anno)

01-SSC-0252 Serie TZ600 (1 anno)

01-SSC-2001 NS*a* 2650 (1 anno)

01-SSC-4030 NS*a* 3650 (1 anno)

01-SSC-4062 NS*a* 4650 (1 anno)

01-SSC-4068 NS*a* 5650 (1 anno)

01-SSC-9131 NS*a* 6600 (1 anno)

** Escluso NSa 9250-9650*

Sono disponibili anche SKU per più anni. Visitare il sito www.sonicwall.com

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

Informazioni su SonicWall

Da oltre 27 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 rilevamento e prevenzione automatizzata delle violazioni in tempo reale ottimizzata per le esigenze specifiche di oltre 500.000 organizzazioni in più di 215 paesi e regioni, per consentire loro di fare più affari con maggior sicurezza.

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

DataSheet-CompAntiSpamService-US-VG-MKTG4092