# Quali sono le procedure ottimali per l'utilizzo di SenderBase?

## Sommario



## Introduzione

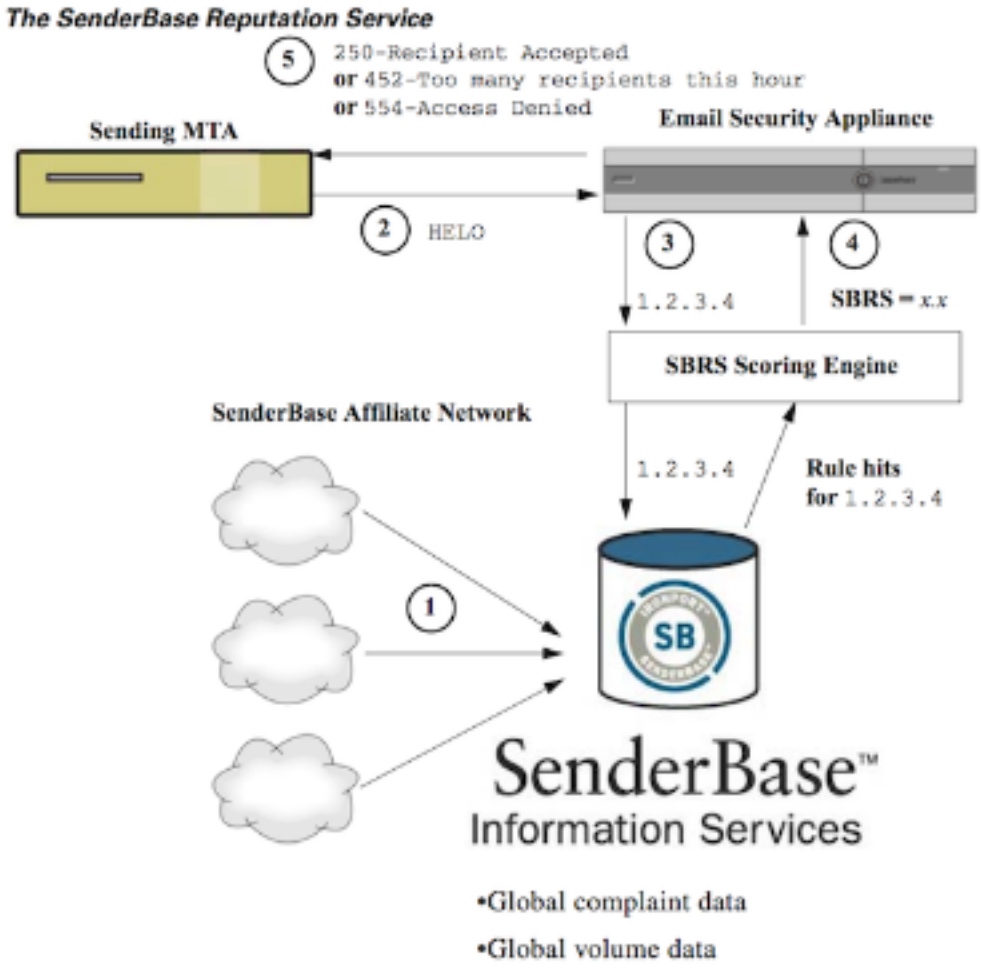
In questo documento vengono descritte le procedure consigliate per l'utilizzo di SenderBase.

## Quali sono le procedure ottimali per l'utilizzo di SenderBase?

Il servizio SenderBase Reputation Service (SBRS) offre un modo preciso e flessibile per rifiutare o limitare i sistemi che potrebbero trasmettere spam in base all'indirizzo IP di connessione dell'host remoto. La funzione SBRS restituisce un punteggio basato sulla probabilità che un messaggio proveniente da una determinata origine sia indesiderato, che va da -10 (sicuramente posta indesiderata) a +10 (sicuramente non posta indesiderata). Sebbene la funzione SBRS possa essere utilizzata come soluzione autonoma anti-spam, risulta più efficace se combinata con uno scanner anti-spam basato sul contenuto.

I punteggi di SenderBase possono essere utilizzati nella tabella HAT (Host Access Table) su un listener SMTP per mappare le connessioni SMTP in ingresso a diversi gruppi di mittenti. Ogni gruppo di mittenti ha associato a esso un criterio che influisce sulla modalità di gestione della posta elettronica in arrivo. I punteggi di SenderBase hanno in genere l'effetto di rifiutare completamente la posta o di limitare il mittente di posta indesiderata sospetto.

Èpossibile utilizzare i punteggi SBRS in HAT per rifiutare o limitare la posta elettronica. È inoltre possibile creare filtri messaggi per specificare "soglie" per i punteggi SBRS in modo da intervenire ulteriormente sui messaggi elaborati dal sistema. Il diagramma seguente offre una descrizione sommaria di come utilizzare i punteggi SBRS per bloccare o limitare i mittenti sospetti:




1. Gli affiliati SenderBase inviano dati globali in tempo reale.
2. L'invio di MTA consente di stabilire una connessione con l'accessorio.
3. L'accessorio controlla i dati globali relativi all'indirizzo IP di connessione.
4. Servizio reputazione SenderBase calcola la probabilità che questo messaggio sia indesiderato e assegna un punteggio reputazione SenderBase.
5. L'accessorio restituisce la risposta (rifiuto dell'e-mail o limitazione del mittente) in base al punteggio di reputazione SenderBase.

Il modo in cui utilizzi i punteggi SBRS dipenderà dalla tua aggressività nel pre-filtrare i messaggi di posta elettronica. Email Security Appliance (ESA) offre tre diverse strategie per l'implementazione di SenderBase:

- **Conservatore**: Un approccio conservativo consiste nel bloccare i messaggi con un punteggio di reputazione SenderBase inferiore a -7,0, impostare un valore compreso tra -7,0 e -2,0, applicare il criterio predefinito tra -2,0 e +6,0 e il criterio di attendibilità per i messaggi con un punteggio superiore a +6,0. Questo approccio garantisce una percentuale di falsi positivi prossima allo zero, migliorando al contempo le prestazioni del sistema.
- **Sufficiente:** Un approccio moderato consiste nel bloccare i messaggi con un punteggio di reputazione di SenderBase inferiore a -4,0, impostare un valore compreso tra -4,0 e 0, applicare il criterio predefinito tra 0 e +6,0 e il criterio attendibile per i messaggi con un punteggio maggiore di +6,0. Questo approccio garantisce una percentuale di falsi positivi molto ridotta e consente di ottenere migliori prestazioni del sistema (in quanto più messaggi vengono allontanati dall'elaborazione della protezione dalla posta indesiderata).
- **Aggressivo:** Un approccio aggressivo consiste nel bloccare i messaggi con un punteggio di reputazione SenderBase inferiore a -1,0, impostare un valore compreso tra -1,0 e 0, applicare

il criterio predefinito tra 0 e +4,0 e il criterio di attendibilità per i messaggi con un punteggio superiore a +4,0. Questo approccio potrebbe determinare il verificarsi di alcuni falsi positivi. tuttavia, questo approccio ottimizza le prestazioni del sistema allontanando la maggior parte dei messaggi dall'elaborazione antispam.

La tabella seguente riassume queste tre politiche:

| Approccio | Caratteristiche | Allowlist | Blocklist | Elenco dei sospetti | Elenco sconosciuto |
|---|---|---|---|---|---|
| | | Intervallo punteggio reputazione base mittente: | | | |
| **Conservatore** | Quasi zero falsi positivi, migliori prestazioni | da 7 a 10 | da -10 a -4 | da -4 a -2 | da -2 a 7 |
| **Sufficiente** (impostazione predefinita) | Pochissimi falsi positivi, prestazioni elevate | I punteggi della reputazione di base del mittente non sono utilizzati. | da -10 a -3 | da -3 a -1 | da -1 a +10 |
| **Aggressivo** | Alcuni falsi positivi, massime prestazioni<br>Questa opzione consente di allontanare la maggior parte dei messaggi dall'elaborazione della protezione da posta indesiderata. | da 4 a 10 | da -10 a -2 | da -2 a -1 | da -1 a 4 |
| Tutti gli approcci | | Criteri flusso di posta: Attendibile | Bloccato | Limitato | Accettato |

# Implementazione della limitazione o del blocco SenderBase

Il modo migliore per utilizzare i punteggi di SenderBase consiste nel seguire una semplice metodologia in due parti. Innanzitutto, si decide il criterio (ad esempio, è possibile iniziare con il criterio "Conservativo" descritto in precedenza) e lo si mappa ai gruppi di mittenti. Mappare quindi tali gruppi di mittenti al criterio desiderato. L'ESA ha già creato una matrice di gruppi di mittenti e di policy di flusso della posta che può servire da modello per l'implementazione di SBRS.

Per implementare la limitazione di SenderBase in base al criterio predefinito, modificare i quattro gruppi di mittenti (Allowlist, Blocklist, Suspectlist e Unknown list) in Criteri di posta > Panoramica tabella Host Access (HAT). Iniziare facendo clic sul gruppo di mittenti "Allowlist". Quindi, utilizzando il menu a discesa nella scheda Mittenti, fare clic su "Aggiungi mittente" con "SenderBase Reputation Score (SBRS)" selezionato. In questo modo verrà aggiunta una riga SBRS all'elenco dei mittenti. Completare l'intervallo di punteggi SBRS (in questo caso da 6.0 a 10) fare clic sul pulsante **Invia**.

Il criterio per il gruppo di mittenti Allowlist è "Attendibile". Per impostazione predefinita, questo criterio ignorerà l'elaborazione della posta indesiderata, migliorando le prestazioni del sistema. Poiché i mittenti con punteggi SBRS molto elevati hanno maggiori probabilità di inviare posta

indesiderata, questo passaggio da solo aumenterà la velocità effettiva. Modificare i tre gruppi di mittenti rimanenti per aggiungere i punteggi SBRS, in base alla tabella seguente:

| Gruppo mittente | Intervallo punteggio | Risultato |
|---|---|---|
| Allowlist | Da 6 a 10 | I mittenti riconosciuti validi non verranno analizzati |
| Elenco sconosciuto | da -2 a +6 | I mittenti con informazioni limitate verranno analizzati normalmente |
| Elenco dei sospetti | da -7 a -2 | I mittenti con reputazione scadente saranno pesantemente limitati per ridurre quantità di spam che possono inviare |
| Blocklist | da -10 a -7 | I messaggi inviati da spammer noti verranno rifiutati al momento di SMTP co risposta di 5xx |

Una volta aggiunti gli intervalli di punteggio, non dimenticare di fare clic su "**Commit modifiche**". Quando si aggiungono regole di punteggio SBRS a gruppi di mittenti esistenti, posizionarli in fondo all'elenco di mittenti in qualsiasi gruppo. L'ordine è importante quando si definiscono i gruppi di mittenti in un HAT del listener, poiché i gruppi vengono valutati dall'alto verso il basso e all'interno di ogni gruppo, ogni regola viene valutata singolarmente, dall'alto verso il basso. In un HAT, la prima regola corrispondente a un mittente verrà utilizzata per selezionare un criterio. Se una connessione in ingresso da un dominio di invio ha un punteggio SBRS definito e corrisponde all'intervallo in una regola nel HAT del listener, verrà applicato il criterio del flusso di posta, anche se potrebbero corrispondere altre regole più in basso nell'elenco dei gruppi di mittenti.

Se il criterio per l'inserimento dei mittenti nei gruppi di mittenti richiede che tutte le regole non SBRS vengano valutate prima di prendere in considerazione i punteggi SBRS, è possibile aggiungere semplicemente quattro nuovi gruppi di mittenti alla fine dell'elenco dei gruppi di mittenti esistenti specificatamente per la corrispondenza al criterio SBRS insieme ai relativi criteri.

## Informazioni correlate

- Domande frequenti su SenderBase
- Documentazione e supporto tecnico – Cisco Systems