Configura elenco eccezioni dominio mittente per Secure Email Gateway

Sommario

Introduzione

In questo documento vengono descritte "Nuove modifiche" apportate all'opzione di impostazione Sender Domain Reputation (SDR), Elenco eccezioni dominio, per Cisco Secure Email Gateway (SEG).

Contributo di Chris Arellano Cisco TAC Engineer.

Prerequisiti

Si desidera una conoscenza generale delle impostazioni e della configurazione di SEG.

AsyncOS 15.0 e versioni successive per Cisco Secure Email Gateway (SEG).

Comprensione generale della funzione SDR.

Requisiti

Abilitare il Servizio reputazione dominio mittente e creare un elenco indirizzi con l'opzione Solo dominio.

Componenti usati

- Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:
  - Cisco Secure Email Gateway (SEG) AsyncOS 15.5.1 e versioni successive.
- Reputazione dominio mittente SEG.
- Elenco indirizzi.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

La reputazione del dominio del mittente è un servizio cloud che raccoglie più valori del mittente, emette verdetti e fornisce opzioni per intervenire su tali verdetti. SDR consente alle impostazioni di ignorare i domini trusted tramite l'utilizzo di un elenco indirizzi applicato all'elenco eccezioni dei domini.

L'elenco delle eccezioni di dominio SDR nelle versioni AsynOS precedenti a SEG 15.0 aveva due opzioni:

- Enabled = Associa busta da, dominio per ignorare l'azione SDR.
- Disabilitata = Corrispondenza solo se sono presenti tutti i valori: Inviluppo da + Invisibile da + Rispondi a + SPF + DKIM + DMARC .

Elenco delle eccezioni di dominio per SEG 15.0 e versioni successive:

- Enabled = Associa busta da, dominio per ignorare l'azione SDR.
- Disabled = Corrispondenza se il dominio è presente in uno dei valori:
    - HELO
    - RDN
    - Busta - Da
    - Da
    - Rispondi a

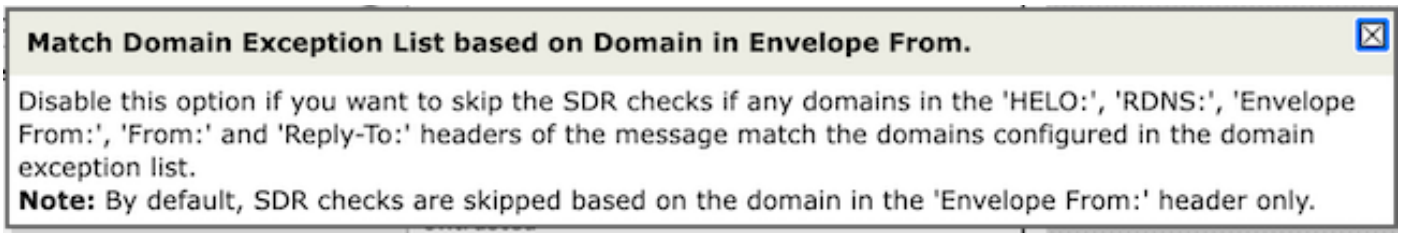
Configurazione

In questo articolo è presente solo la nuova configurazione dell'elenco eccezioni dei domini. La configurazione e l'impostazione completa dell'SDR sono fornite nel Manuale dell'utente.

Spostarsi all'interno di WebUI in Security Services > Domain Reputation (Servizi di sicurezza > Reputazione dominio).

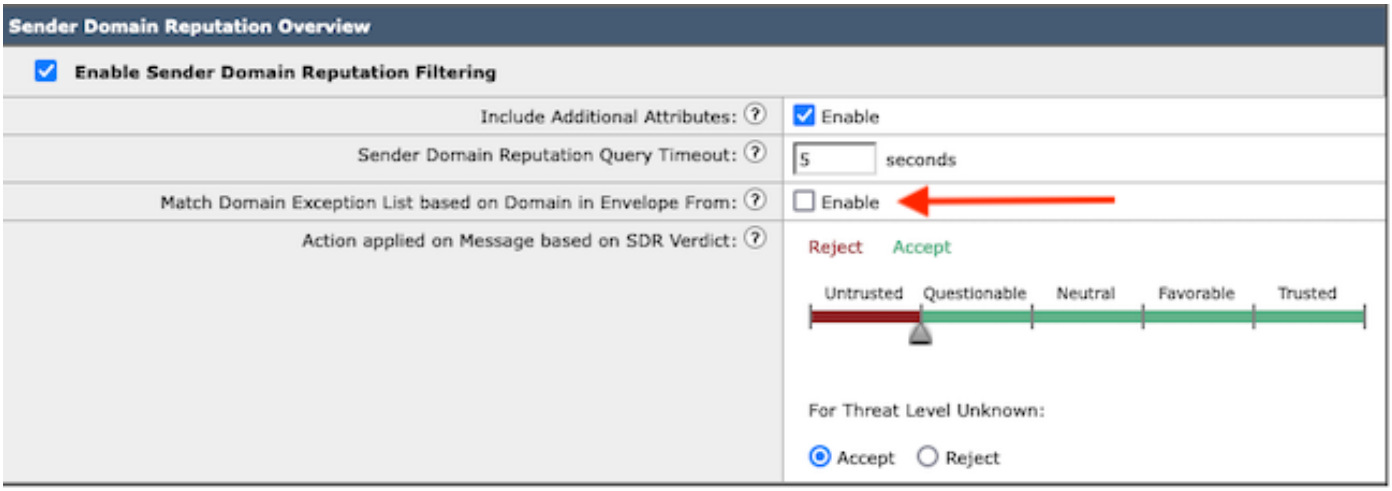
- L'opzione Corrispondenza elenco eccezioni dominio basata sulla parte Nome dominio della busta Da è abilitata per impostazione predefinita.
    - Se la casella di controllo è attivata, solo il valore "Busta da, intestazione" corrisponderà e ignorerà il messaggio se condannato.
    - Se la casella di controllo è vuota, SDR Domain Exception List corrisponderà a uno qualsiasi di questi campi di intestazione 'HELO:', 'RDNS:', 'Envelope From:', 'From:' e 'Reply-To:', corrisponderà e ignorerà il messaggio se condannato.

Se è selezionata l'icona ? informativa associata, vengono visualizzati i dettagli dell'impostazione.



Nota: per impostazione predefinita, i controlli SDR vengono ignorati in base al dominio specificato solo nell'intestazione 'Inviluppo da:'.

Selezionare Modifica impostazioni globali per rimuovere l'opzione della casella di controllo, come mostrato nell'immagine:



Lo stesso elenco di eccezioni di dominio è un elenco di indirizzi contenente nomi di dominio.

Verifica

Per verificare il corretto funzionamento utilizzando la nuova funzionalità Disable, è necessario inviare un messaggio di prova al SEG con un valore di dominio corrispondente in uno dei 5 valori dell'intestazione.

Un log di esempio che indica un'eccezione all'interno dell'Elenco eccezioni globale e corrispondente all'interno di un criterio del flusso di posta viene presentato nella fase iniziale ai log di posta:

```
Info: MID 14 SDR: MID 14 containing domain name'test1.example.com' matched the global domain exception
```

Un registro di esempio che indica un'eccezione conterrà sia il nome del dominio che il nome dell'elenco di eccezioni.

```
Info: MID 16 containing domain name 'test3.example.com' matched the domain exception list 'SDR-TEST-3'
```

Risoluzione dei problemi

In caso di domande sull'accuratezza del verdetto di un messaggio selezionato, i valori vengono documentati e confrontati con la verifica del messaggio.

- Documentare le Impostazioni reputazione dominio globale > Impostazioni protezione > Reputazione dominio.
- Verificare l'elenco indirizzi associato configurato nelle impostazioni di reputazione del dominio globale.
- Verificare il criterio del flusso di posta corrispondente in base alla verifica dei messaggi.
- Controllare e annotare i dettagli dei filtri messaggi o dei filtri contenuti con elenchi di eccezioni di dominio configurati.

Raccogli verifica messaggi, log di posta e intestazioni di posta elettronica originali.

- Se l'eccezione Globale corrisponde a un messaggio, non esistono voci di registro per la Reputazione del dominio, ma semplicemente una riga che indica il dominio corrispondente.
- Se l'Elenco eccezioni globale non corrisponde in un messaggio, esistono voci di log per la reputazione del dominio da cui confrontare i valori.
    - Informazioni: MID 16 SDR: Domini per i quali è richiesto SDR: reverse DNS host: Not Present, helo: mail1.example.com, env-from: test2.example.com, header-from: te destination.example.com, rispondere a: test2.example.com
- Le intestazioni dei messaggi di posta elettronica includono uno qualsiasi dei 5 valori presenti in un singolo messaggio di posta elettronica da confrontare con le impostazioni.

Una volta raccolti tutti i dati, verificare la presenza di corrispondenze o l'assenza di corrispondenze per determinare la funzionalità corretta.

Informazioni correlate

- Guida alla configurazione di Email Security
- Pagina di avvio di Cisco Secure Email Gateway per il supporto delle guide

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).