Configurazione di SPF e best practice

Sommario

Introduzione

Questo documento descrive diversi scenari con Sender Policy Framework (SPF) su Cisco Email Security Appliance (ESA).

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ESA
- Tutte le versioni di AsyncOS

Che cos'è SPF?

Sender Policy Framework (SPF) è un semplice sistema di convalida della posta elettronica progettato per rilevare lo spoofing della posta elettronica fornendo un meccanismo che consente agli scambiatori di posta di ricevere la posta in arrivo da un dominio e di controllare che la posta in arrivo venga inviata da un host autorizzato dagli amministratori del dominio. L'elenco degli host di invio autorizzati per un dominio viene pubblicato nei record DNS (Domain Name System) del dominio sotto forma di record TXT con formattazione speciale. La posta indesiderata e il phishing utilizzano spesso indirizzi di mittenti falsi, pertanto la pubblicazione e il controllo dei record SPF possono essere considerati tecniche anti-spam.

Le ESA avranno un notevole impatto sulle prestazioni?

Dal punto di vista della CPU, non ci sarà un impatto enorme sulle prestazioni. Tuttavia, l'attivazione della verifica SPF aumenterà il numero di query DNS e il traffico DNS. Per ogni messaggio, è possibile che l'ESA debba avviare 1-3 query DNS SPF. In questo modo la cache DNS scadrà prima del precedente. Pertanto, l'ESA genererà un numero maggiore di query anche

per gli altri processi.

Oltre alle informazioni precedenti, il record SPF sarà un record TXT che potrebbe essere più grande dei normali record DNS e causare traffico DNS aggiuntivo.

Come si attiva l'SPF?

Le seguenti istruzioni sono contenute nella Guida dell'utente avanzata per l'impostazione della verifica SPF:

Per abilitare SPF/System Independent Data Format (SIDF) nel criterio di flusso di posta predefinito:

1. Fare clic su **Mail Policies > Mail Flow Policy (Policy di posta > Criteri flusso di posta)**.
2. Fare clic su **Parametri criteri predefiniti**.
3. Nei parametri dei criteri predefiniti visualizzare la sezione **Funzionalità di sicurezza**.
4. Nella sezione Verifica SPF/SIDF fare clic su **Sì**.
5. Impostare il livello di conformità (il valore predefinito è compatibile con SIDF). Questa opzione consente di determinare lo standard di verifica SPF o SIDF da utilizzare. Oltre alla conformità SIDF, è possibile scegliere la compatibilità SIDF, che combina SPF e SIDF. I dettagli sui livelli di conformità sono disponibili nella *Guida dell'utente finale.*
6. Se si sceglie un livello di conformità compatibile con SIDF, configurare se la verifica declassa il risultato **Pass** dell'identità PRA a **None** se è presente Resent-Sender: o inviato da: intestazioni presenti nel messaggio. È possibile scegliere questa opzione per motivi di sicurezza.
7. Se si sceglie un livello di conformità di SPF, configurare se eseguire un test in base all'identità HELO. È possibile utilizzare questa opzione per migliorare le prestazioni disattivando il controllo HELO. Questa operazione può essere utile perché la regola di filtro passata tramite spf controlla prima le identità PRA o MAIL FROM. L'accessorio esegue solo il controllo HELO per il livello di conformità SPF.

Per eseguire un'azione sui risultati della verifica SPF, aggiungere uno o più filtri contenuti:

1. Creare un filtro del contenuto di stato-spf per ogni tipo di verifica SPF/SIDF. Utilizzare una convenzione di denominazione per indicare il tipo di verifica. Ad esempio, utilizzare **SPF-Passed** per i messaggi che superano la verifica SPF/SIDF o **SPF-TempErr** per i messaggi che non sono stati superati a causa di un errore temporaneo durante la verifica. Per informazioni sulla creazione di un filtro del contenuto spf-status, vedere la regola di filtro del contenuto spf-status nell'interfaccia utente grafica.
2. Dopo aver elaborato alcuni messaggi verificati per SPF/SIDF, fare clic su **Monitor > Content Filters** (Filtri contenuti) per visualizzare il numero di messaggi che hanno attivato ciascuno dei filtri contenuti verificati per SPF/SIDF.

Cosa significa "Helo Test" acceso e spento? Cosa succede se il test di Helo non viene eseguito in un determinato dominio?

Se si sceglie un livello di conformità di SPF, configurare se eseguire un test in base all'identità

HELO. È possibile utilizzare questa opzione per migliorare le prestazioni disattivando il controllo HELO. Questa operazione può essere utile perché la regola di filtro passata tramite spf controlla prima le identità PRA o MAIL FROM. L'accessorio esegue solo il controllo HELO per il livello di conformità SPF.

Record SPF validi

Per superare il controllo SPF HELO, assicurarsi di includere un record SPF per ogni MTA di invio (separato dal dominio). Se non includi questo record, il controllo HELO produrrà probabilmente un verdetto **None** per l'identità HELO. Se i mittenti SPF nel tuo dominio restituiscono un numero elevato di verdetti **None**, è possibile che questi mittenti non abbiano incluso un record SPF per ogni MTA di invio.

Il messaggio verrà recapitato se non sono configurati filtri messaggi/contenuti. Anche in questo caso, è possibile eseguire determinate azioni utilizzando i filtri messaggi/contenuti per ogni verdetto SPF/SIDF.

Qual è il modo migliore per abilitarlo per un solo dominio esterno?

Per abilitare l'SPF per un determinato dominio, potrebbe essere necessario definire un nuovo gruppo di mittenti con un criterio del flusso di posta in cui SPF è abilitato; quindi creare i filtri come indicato in precedenza.

Èpossibile abilitare un SPF per il controllo della posta indesiderata?

La funzionalità Cisco Anti-Spam considera una serie di fattori per calcolare i punteggi della posta indesiderata. La presenza di un record SPF verificabile può ridurre il punteggio della posta indesiderata, ma esiste ancora la possibilità di ottenere tali messaggi identificati come posta indesiderata sospetta.

La soluzione migliore sarebbe quella di consentire l'elenco dell'indirizzo IP del mittente O creare un filtro messaggi per ignorare il controllo della posta indesiderata con più condizioni (ip remoto, da e-mail, intestazione X-skipspamcheck, ecc.). L'intestazione può essere aggiunta dal server di invio per identificare un tipo di messaggi da altri.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Procedure ottimali per l'autenticazione e-mail - Implementazione di SPF/DKIM/DMARC
- Documentazione e supporto tecnico – Cisco Systems