Come configurare l'ESA in modo che ignori la scansione antispam e/o antivirus per i mittenti attendibili?

Sommario

[Domanda](#)
[Risposta](#)
[Informazioni correlate](#)

Domanda

Come configurare l'ESA in modo che ignori la scansione antispam e/o antivirus per i mittenti attendibili?

Risposta

AsyncOS offre tre strumenti principali che è possibile utilizzare per ignorare il controllo antispam o antivirus per i mittenti più attendibili. Si noti che l'ESA non consiglia di saltare il controllo antivirus in qualsiasi momento, anche per i mittenti più affidabili, a causa del potenziale di infezioni involontarie da virus. Di seguito vengono illustrati i tre modi in cui è possibile ignorare il controllo della posta indesiderata per un sottoinsieme del flusso di messaggi.

Il primo strumento disponibile è Host Access Table (HAT) Mail Flow Policies. Tramite i criteri di flusso della posta è possibile identificare i mittenti in base all'indirizzo IP (utilizzando indirizzi IP numerici o nomi DNS PTR), al punteggio di SenderBase o a un elenco di indirizzi DNS consentiti o un elenco di indirizzi bloccati locale. Dopo aver identificato i mittenti come attendibili all'interno di un gruppo di mittenti in HAT, è possibile contrassegnare tale gruppo di mittenti per ignorare l'analisi della posta indesiderata.

Si supponga, ad esempio, di voler identificare un partner commerciale specifico, EXAMPLE.COM, che non deve disporre del controllo antispam sulla posta. È necessario conoscere gli indirizzi IP del server di posta di SCU.COM (o i record dei puntatori DNS). In questo caso, supponiamo che EXAMPLE.COM abbia server di posta che avranno indirizzi IP con record PTR DNS da "smtp1.mail.scu.com" a "smtp4.mail.scu.com". Ricordare in questo caso che stiamo esaminando il record PTR (talvolta denominato DNS inverso) per i server di posta; questa operazione non ha nulla a che fare con il nome di dominio che gli utenti all'indirizzo SCU.COM utilizzeranno per la posta in uscita.

Èpossibile creare un nuovo gruppo di mittenti (o utilizzare un gruppo di mittenti esistente, ad esempio ALLOWLIST) con Criteri di posta>Panoramica>Aggiungi gruppo di mittenti. Creiamone uno chiamato "NotSpammers". Dopo aver inviato questa pagina, tornerai alla schermata Criteri di posta>Panoramica, in cui potrai aggiungere un nuovo criterio per questo gruppo di mittenti. Se fai clic su "Aggiungi criterio", ti verrà data l'opportunità di creare un nuovo criterio. In questo caso, si desidera sostituire il criterio predefinito solo in un'area: Rilevamento posta indesiderata. Assegnare un nome al criterio e impostare il comportamento della connessione su "Accetto", quindi scorrere verso il basso fino alla sezione Rilevamento posta indesiderata e impostare il

criterio in modo da ignorare il controllo della posta indesiderata. Inviare il nuovo criterio e non dimenticare di eseguire il commit delle modifiche.

Un approccio alternativo consiste nell'utilizzare le policy di posta in arrivo per ignorare l'analisi della posta indesiderata. La differenza tra i criteri HAT e Posta in arrivo consiste nel fatto che il criterio HAT si basa interamente sulle informazioni IP del mittente: l'indirizzo IP reale, l'indirizzo IP riflesso nel DNS, il punteggio SenderBase (basato sull'indirizzo IP) o una voce DNS allowlist o blocklist basata sull'indirizzo IP. I criteri della posta in arrivo si basano sulle informazioni sulla busta del messaggio: il destinatario o l'origine del messaggio. Ciò significa che possono essere ingannati dalla rappresentazione di un mittente del messaggio. Tuttavia, se si desidera semplicemente ignorare tutti i controlli della posta indesiderata provenienti da utenti con indirizzi di posta elettronica che terminano con "@example.com", è possibile eseguire anche questa operazione.

Per creare un criterio di questo tipo, scegliere **Mail Policies > Incoming Mail Policies > Add Policy** (Policy di posta in arrivo > Aggiungi criterio). In questo modo sarà possibile aggiungere un criterio che definisca un set di mittenti (o destinatari). Una volta definito, il criterio Posta in arrivo verrà visualizzato nella schermata di panoramica (Criteri di posta>Criteri posta in arrivo). È quindi possibile fare clic sulla colonna "Anti-Spam" e modificare le impostazioni specifiche per la protezione da posta indesiderata per questo particolare utente.

Le impostazioni della protezione dalla posta indesiderata per un criterio specifico possono essere configurate in numerose opzioni, ma in questo caso è sufficiente ignorare il controllo della protezione. Si noti un'altra differenza tra i criteri basati su HAT e i criteri della posta in arrivo: HAT consente solo di ignorare o non ignorare la scansione della posta indesiderata, mentre i criteri della posta in arrivo offrono un controllo maggiore. È ad esempio possibile scegliere di mettere in quarantena le e-mail indesiderate provenienti da determinati mittenti ed eliminare quelle provenienti da altri mittenti.

La terza opzione per ignorare l'analisi della posta indesiderata è la configurazione e l'utilizzo di un filtro messaggi.

> **Nota:** Impossibile utilizzare i filtri contenuti. I filtri contenuti vengono applicati dopo l'analisi della posta indesiderata

Una delle azioni disponibili in Filtri messaggi è "skip-spamcheck". Il filtro messaggi seguente ignora il controllo della posta indesiderata per i mittenti con un indirizzo IP specifico o che provengono da un nome di dominio specifico:

```
SkipSpamcheckFilter:
   if ( (remote-ip == '192.168.195.101') or
        (mail-from == '@example\\.com$')      )
   {
       skip-spamcheck();
   }
```

Per ulteriori informazioni sull'utilizzo dei filtri messaggi, consultare la Guida dell'utente per la versione di AsyncOS distribuita.

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems