Errori comuni di configurazione sull'ESA

Sommario

[Introduzione](#)
[Quali sono gli errori di configurazione comuni sull'ESA?](#)
[CAPPELLO](#)
[Policy](#)
[Relay in ingresso](#)
[DNS](#)
[Filtri messaggi e contenuti](#)
[Prevenzione inoltro aperto](#)
[Informazioni correlate](#)

Introduzione

In questo documento vengono descritti gli errori di configurazione comuni di Email Security Appliance (ESA).

Quali sono gli errori di configurazione comuni sull'ESA?

Sia che si stia impostando una nuova valutazione o si stia cercando una configurazione esistente, è possibile fare riferimento a questo elenco di controllo degli errori di configurazione comuni.

CAPPELLO

- Non inserire punteggi positivi SBRS come +5 o +7 nell'ELENCO CONSENTITI. Un intervallo compreso tra 9,0 e 10,0 è corretto, ma l'inclusione di punteggi più bassi renderà solo più probabile il superamento della posta indesiderata.
- Disabilitare UNKNOWNLIST, Envelope Sender DNS Verification e Connecting Host DNS Verification a meno che non siano effettivamente necessari e comprensibili.
- Anziché modificare le dimensioni dei messaggi e altre impostazioni dei criteri in ogni criterio di flusso della posta, passare al menu Criteri di flusso della posta e scegliere l'ultima opzione, "Parametri criteri predefiniti".
- Limita a tre il numero massimo di connessioni per la maggior parte dei mittenti e imposta questa impostazione come predefinita per i nuovi criteri di flusso della posta.
- Verificare che i punteggi di SenderBase da -10,0 a -2,0 siano inclusi nell'elenco di blocco. La documentazione e le procedure guidate di configurazione sono eccessivamente conservative; attualmente non sono presenti falsi positivi in questo intervallo.

Policy

- Denominare le politiche dopo chi le ottiene, non quello che fanno. Assegnare un nome ai filtri dei contenuti dopo le operazioni eseguite e utilizzare abbreviazioni quali

Q_basic_attachments, D_spoofers, Strip_Multi-Media, dove Q indica la quarantena e D indica la perdita.
- Le policy non predefinite devono utilizzare le impostazioni predefinite per i filtri antispam, antivirus, dei contenuti e epidemie, ad eccezione dei casi in cui sono necessarie impostazioni speciali. Non ricreare tali impostazioni in ogni criterio se non è necessario.
- Deselezionare "Elimina allegati infetti" altrimenti si passeranno molte email vuote dove il virus è stato rimosso.
- Le impostazioni antivirus per il traffico in uscita devono informare il mittente, non il destinatario
- I filtri epidemie e la protezione dalla posta indesiderata devono essere disabilitati in uscita

Relay in ingresso

Se in "Monitor > Overview" vengono visualizzate le connessioni dai propri server e domini, è necessario aggiungerle all'impostazione Incoming Relays. Un errore molto comune, quando si utilizza la GUI, è quello di pensare che la funzione Incoming Relay sia stata abilitata dopo aver aggiunto le voci alla tabella. Inoltre:

- Aggiungere un gruppo di mittenti HAT speciale per loro, sopra ALLOWLIST, per scopi di report. Scegliere nessuna limitazione di velocità o DHCP, ma il rilevamento di spam e virus è corretto.
- Aggiungere un filtro messaggi corrispondente all'azione del criterio BLOCKLIST. Ad esempio:

```
Drop_Low_Reputation_Relayed_Mail:
if reputation <= -2.0
{ drop();}
```

Nei rari casi in cui si sta reinserendo la posta elettronica (ad esempio, rielaborando la posta tra gli abbonati tramite la policy della posta in arrivo), il filtro dovrà esentare anche l'interfaccia di reinserimento. Normalmente questo non è necessario.

DNS

Molti clienti forzano l'ESA a interrogare i propri server DNS interni fuori dall'abitudine. Nella maggior parte delle installazioni, il 100% dei record DNS necessari si trova su Internet e non nel DNS interno. È consigliabile eseguire query sui server radice Internet, riducendo il carico di inoltro sul DNS interno.

Filtri messaggi e contenuti

L'errore più comune consiste nell'inserire condizioni corrispondenti nei filtri contenuti dove non sono necessarie. La maggior parte dei filtri deve elencare alcune azioni, ma la condizione deve essere lasciata vuota. Il filtro sarà *true* sempre e verrà eseguito sempre. È possibile controllare gli utenti/criteri che ricevono queste azioni creando nuovi criteri di posta in arrivo o in uscita in base alle esigenze e applicando questo filtro al criterio. Ecco alcuni esempi errati e corretti:

- L'utilizzo della condizione rcpt-to in un filtro messaggi è quasi sempre un errore. La procedura corretta consiste nello scrivere un filtro dei contenuti in arrivo e renderlo specifico per un utente specifico aggiungendo un criterio di posta in arrivo basato sul destinatario.

- Èquasi sempre un errore verificare la presenza di un allegato mediante un filtro dei contenuti, quindi eliminare l'allegato. Il metodo corretto consiste nell'eliminare sempre l'allegato senza verificarne la presenza.
- L'utilizzo di delivery() è quasi sempre un errore. Consegna significa ignorare i filtri rimanenti, quindi consegnare. Se si desidera eseguire il recapito senza ignorare il resto dei filtri, non è richiesta alcuna azione esplicita (recapito implicito).

Prevenzione inoltro aperto

Alcuni servizi verificheranno se il proprio agente di trasferimento messaggi (MTA) accetta indirizzi che potrebbero determinare condizioni di inoltro aperto. Poiché lasciare l'MTA come inoltro aperto funzionante non è corretto, questi siti potrebbero aggiungere l'utente a un BLOCKLIST a meno che questi indirizzi pericolosi non vengano rifiutati nella conversazione SMTP.

Aggiungere un gruppo di mittenti HAT speciale per loro, sopra ALLOWLIST, per scopi di report. Scegliere nessuna limitazione di velocità o DHCP, ma consentire il rilevamento di spam e virus.

- Passa all'analisi degli indirizzi rigidi (l'impostazione predefinita è Loose). Ciò è necessario per evitare doppi segni @ negli indirizzi.
- Rifiuta (non rimuove) i caratteri non validi. Ciò è necessario anche per evitare doppi segni @ negli indirizzi.
- Rifiutare (non accettare) valori letterali e immettere i caratteri seguenti: *%!\\/?

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems