Come è possibile evitare la crittografia in un filtro dei contenuti e in un DLP?

Sommario

[Introduzione](#)
[Come è possibile evitare la crittografia in un filtro dei contenuti e in un DLP?](#)
[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come ignorare la crittografia in un filtro contenuti e in un DLP.

Come è possibile evitare la crittografia in un filtro dei contenuti e in un DLP?

Su Cisco Email Security Appliance (ESA), si dispone di un ambiente che deve essere crittografato in base a un campo soggetto e ai criteri di prevenzione della perdita dei dati. In alcune istanze si desidera ignorare entrambi i trigger di crittografia per un messaggio.

1. Creare un filtro dei contenuti in uscita che preceda quello che esegue la crittografia. Dall'interfaccia grafica **Policy di posta > Filtri contenuti in uscita > Aggiungi filtri...**
2. La condizione consisterà nella ricerca della parola chiave "[NOENCRYPT]" nell'oggetto. Scegliere **Aggiungi condizione...** e selezionare **Subject Header**, con "Contains" \[NOENCRYPT\]. (Le "\" sono per l'uso letterale di "[", quindi immetterle.)
3. La prima azione consiste nell'aggiungere un tag messaggio e il relativo valore è "NOENCRYPTION". (verrà utilizzato nei passaggi successivi dei criteri di prevenzione della perdita dei dati).
4. Infine, l'ultima azione consiste nell'ignorare i filtri dei contenuti rimanenti (azione finale). Si noti che questo filtro e il filtro di crittografia devono essere gli ultimi due nell'elenco degli ordini e questo filtro precede il filtro del contenuto di crittografia. L'aspetto dovrebbe essere simile al seguente:

Conditions

Add Condition...

Order	Condition	Rule	Delete
1	Subject Header	subject == "\\[NOENCRYPT\\]"	

Actions

Add Action...

Order	Action	Rule	Delete
1	Add Message Tag	tag-message ("NOENCRYPTION")	
2	Skip Remaining Content Filters (Final Action)	skip-filters()	

5. Inviare e confermare le modifiche.
6. Dall'interfaccia grafica **Criteri di posta > Criteri posta in uscita**, fare clic su filtro contenuti

(abilita se disabilitato) e selezionare il nuovo filtro contenuti per abilitarlo.

7. Dall'interfaccia grafica, **Policy di posta > Gestione criteri di prevenzione della perdita dei dati** fare clic sui criteri di prevenzione della perdita dei dati esistenti che eseguono la crittografia.
8. Scorrere verso il basso fino a visualizzare *Filtra tag messaggi* e immettere **NESSUNA CRITTOGRAFIA** nel campo e dall'elenco a discesa scegliere *assente* accanto a esso da discesa. Se questo valore è assente, eseguire la crittografia, altrimenti ignorare la crittografia.
9. Invia e conferma il tuo modifiche.

Informazioni correlate

- Cisco Email Security Appliance - Guide per l'utente
- Documentazione e supporto tecnico – Cisco Systems