Guida alle best practice per la prevenzione della perdita dei dati e la crittografia

Sommario

Introduzione
Prerequisiti
Requisiti
Componenti usati
Premesse
Guida alle best practice per la prevenzione della perdita dei dati e la crittografia
1. Abilitare Cisco IronPort Email Encryption sulle ESA
2. Registrare le ESA e l'organizzazione con RES
3. Creazione di profili di cifratura sulle ESA
4. Abilitazione della prevenzione della perdita dei dati
5. Creazione di azioni messaggio di prevenzione della perdita di dati
6. Creazione di politiche di prevenzione della perdita dei dati
7. Applicazione dei criteri di prevenzione della perdita dei dati a un criterio e-mail in uscita
Conclusioni
Informazioni correlate

Introduzione

In questo documento vengono descritte le best practice per la prevenzione delle perdite di dati (DLP) e la crittografia per Cisco Email Security.

In questo documento viene descritta la configurazione della crittografia dei messaggi con Cisco Email Security Appliance (ESA) e Cisco Registered Envelope Service (RES) basato su cloud. I clienti possono utilizzare la crittografia dei messaggi per inviare singoli messaggi in modo sicuro tramite Internet, utilizzando vari tipi di policy, tra cui il filtro dei contenuti e DLP. La creazione di queste politiche sarà discussa in altri documenti all'interno di questa serie. Questo documento si concentra sulla preparazione dell'ESA all'invio di messaggi crittografati in modo che le policy possano utilizzare la crittografia come azione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

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.

Premesse

In questo documento verranno illustrati i seguenti passaggi:

1. Abilitazione di Cisco IronPort Email Encryption
2. Registrazione delle ESA e dell'organizzazione con RES
3. Creazione di profili di crittografia
4. Abilitazione di DLP
5. Creazione di azioni messaggio DLP
6. Creazione di criteri di prevenzione della perdita dei dati
7. Applicazione dei criteri di prevenzione della perdita dei dati a un criterio e-mail in uscita

Una volta completati questi passaggi, l'amministratore ESA può creare una policy che utilizzerà la cifratura come azione.

Cisco IronPort Email Encryption è anche nota come crittografia RES. RES è il nome che utilizziamo per i "server chiave" in Cisco Cloud. La soluzione di crittografia RES utilizza la crittografia a chiave simmetrica, ovvero la chiave utilizzata per crittografare il messaggio è la stessa utilizzata per decrittografare il messaggio. Ogni messaggio crittografato utilizza una chiave univoca, che consente al mittente di avere un controllo granulare su un messaggio dopo l'invio, ad esempio per bloccarlo o scadere in modo che il destinatario non possa più aprirlo, senza influire su altri messaggi. Quando cripta un messaggio, l'ESA memorizza la chiave di cifratura e i metadati nel CRES su ciascun messaggio cifrato.

L'ESA può decidere di criptare un messaggio in molti modi — attraverso il "flag" (come il contenuto del soggetto), attraverso la corrispondenza del filtro contenuti, o attraverso le politiche di prevenzione della perdita dei dati, per esempio. Una volta che l'ESA decide di crittografare un messaggio, lo fa con un "Profilo di crittografia" specificato, creato in "Security Services > Cisco IronPort Email Encryption" — la tabella chiamata "Profilati di crittografia e-mail". Per impostazione predefinita, non esistono profili di crittografia. Questo argomento verrà trattato in *3. Creazione dei profili di crittografia*.

Guida alle best practice per la prevenzione della perdita dei dati e la crittografia

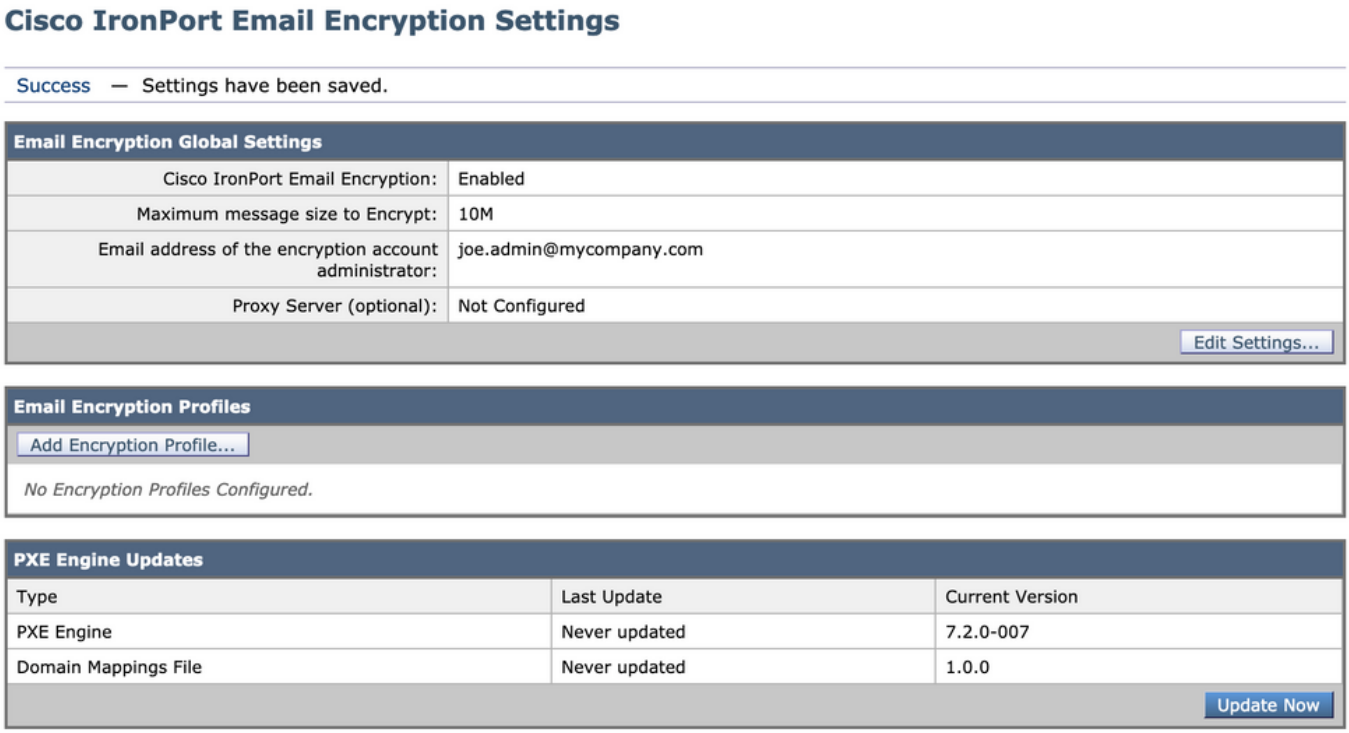
1. Abilitare Cisco IronPort Email Encryption sulle ESA

> **Nota:** Se in un cluster sono presenti più ESA, il passaggio 1 deve essere eseguito una sola volta, poiché queste impostazioni sono in genere gestite a livello di cluster. Se si dispone di più computer non raggruppati o se si gestiscono queste impostazioni a livello di computer, il passo #1 deve essere eseguito su ciascuna ESA.

1. Dall'interfaccia utente dell'ESA, selezionare **Security Services > Cisco IronPort Email Encryption**.
2. Selezionare la casella per abilitare Cisco IronPort Email Encryption.

3. Accettare il contratto di licenza con l'utente finale (EULA) e il contratto di licenza di Cisco IronPort Email Encryption.
4. Nelle *Impostazioni globali di Crittografia e-mail*, fare clic su **Modifica impostazioni...** Specificare l'indirizzo di posta elettronica dell'amministratore o della persona che rappresenta l'amministratore principale di Servizi di risoluzione dei problemi per l'account. Questo account di posta elettronica verrà associato all'amministrazione dell'ambiente RES per la società.Facoltativo: La dimensione massima predefinita dei messaggi da crittografare è 10 MB. Se lo si desidera, è possibile aumentare o ridurre le dimensioni in questo momento.Facoltativo: Se si dispone di un proxy che l'ESA dovrà passare per collegarsi a RES tramite HTTPS, aggiungere le impostazioni proxy e di autenticazione necessarie per consentirne il passaggio attraverso il proxy.
5. Inviare e confermare le modifiche alla configurazione.

A questo punto dovrebbe essere visualizzato il "Email Encryption Global Settings" impostato su qualcosa di simile, ma senza profili ancora elencati:



2. Registrare le ESA e l'organizzazione con RES

Il passo n. 2 viene eseguito principalmente all'esterno della console di amministrazione ESA.

> **Nota:** Le informazioni di registrazione ESA sono disponibili anche nella seguente nota tecnica: [RIS Cisco: Esempio di configurazione ESA Virtual, Hosted e Hardware]

Inviare un'e-mail direttamente a RES: stg-cres-provisioning@cisco.com.

Per effettuare il provisioning di un account CRES per i profili di crittografia dell'ESA, si prega di fornirci le seguenti informazioni:

1. Nome dell'account **(specificare il nome esatto della società, in quanto è necessario che**

venga elencato). Per Cloud Email Security (CES)/account cliente ospitati, annotare il nome del tuo account in modo che termini come "<Nome account> HOSTED"
2. Indirizzi di posta elettronica da utilizzare per l'account amministratore **(specificare l'indirizzo di posta elettronica dell'amministratore corrispondente)**
3. Numero/i di serie completo/i dell'accessorio Il numero di serie di un accessorio può essere individuato dalla GUI ESA (System Administration > Feature Keys) o dalla CLI ESA con il comando "version". Non è accettabile fornire una licenza VLAN (Virtual License Number) o PAK (Product Activitation Key), in quanto per l'amministrazione degli account CRES è necessario specificare un numero di serie completo dell'accessorio.
4. Nomi di dominio da mappare all'account CRES per scopi amministrativi

Nota: Se si dispone già di un account CRES, fornire il nome della società o il numero di account CRES esistente. In questo modo, tutti i nuovi numeri di serie degli accessori verranno aggiunti al conto corretto ed eviteranno la duplicazione delle informazioni aziendali e del provisioning.

Se ricevi un'e-mail relativa al provisioning di un account CRES, ti risponderemo entro un (1) giorno lavorativo. Per supporto e assistenza immediati, aprire una richiesta di supporto con Cisco TAC. A tale scopo, è possibile contattare il Support Case Manager (https://mycase.cloudapps.cisco.com/case) o telefonicamente (https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html).

> **Nota:** Dopo aver inviato questa richiesta tramite e-mail, la creazione dell'account RES della società (se non è già stato creato) e l'aggiunta degli S/N potrebbero richiedere un giorno. L'attività "Provisioning", al passaggio 3, non funzionerà fino al completamento di questa operazione.

3. Creazione di profili di cifratura sulle ESA

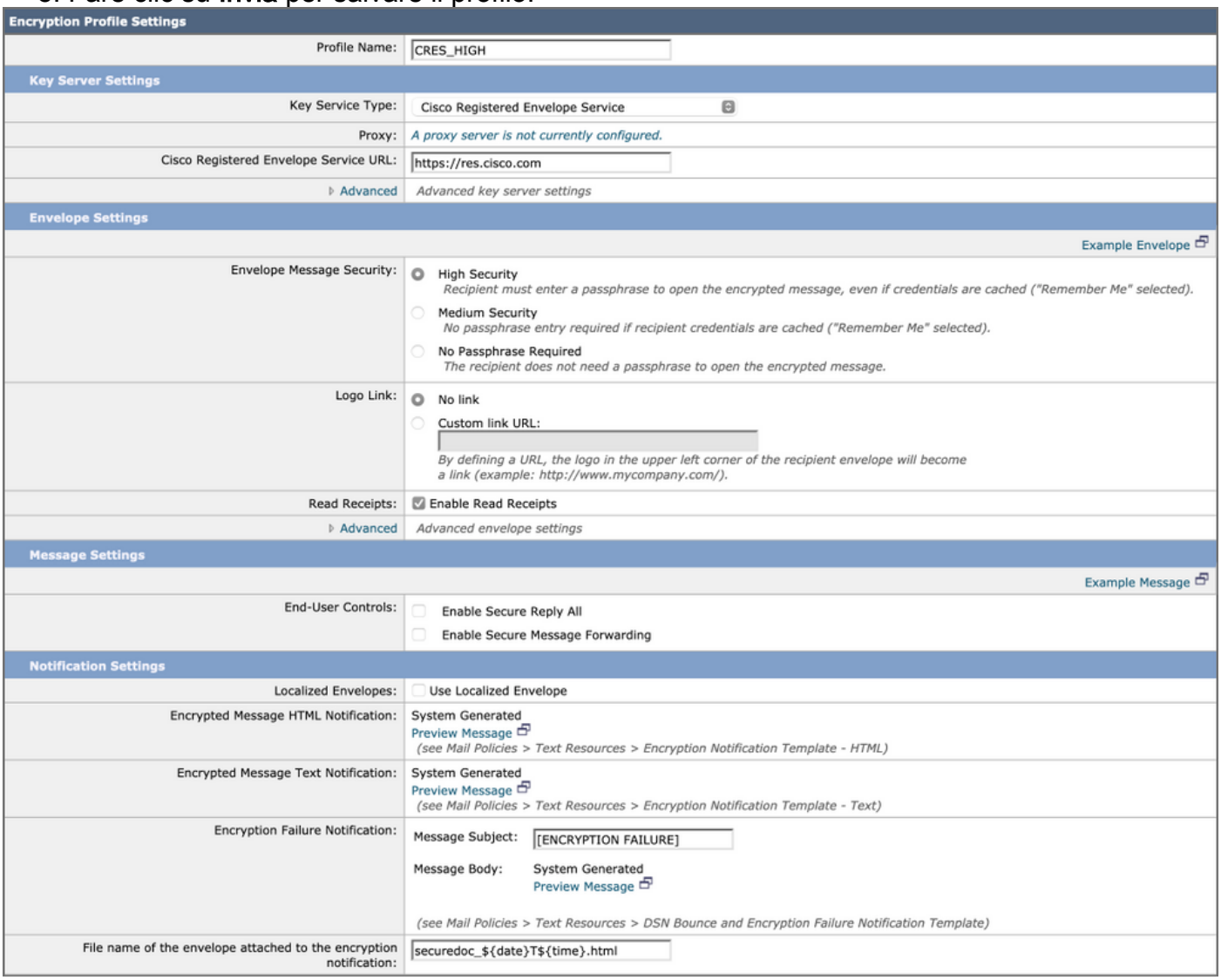
> **Nota:** Se in un cluster sono presenti più ESA, il passaggio 1 deve essere eseguito una sola volta, poiché queste impostazioni sono in genere gestite a livello di cluster. Se si dispone di più computer non raggruppati o se si gestiscono queste impostazioni a livello di computer, il passo #1 deve essere eseguito su ciascuna ESA.

Un profilo di crittografia specifica la modalità di invio dei messaggi crittografati. Ad esempio, un'organizzazione potrebbe dover inviare buste ad alta protezione per un segmento dei destinatari, ad esempio quelli che sanno che invieranno frequentemente dati altamente riservati. La stessa organizzazione può avere altri segmenti della comunità di destinatari che ricevono informazioni meno riservate e che sono forse meno pazienti di fornire ID utente e password per ricevere messaggi crittografati. Tali destinatari sarebbero buoni candidati per un tipo di busta a bassa sicurezza. La presenza di più profili di crittografia consente all'organizzazione di adattare il formato dei messaggi crittografati al pubblico. D'altra parte, molte organizzazioni possono utilizzare un solo Profilo di crittografia.

In questo documento verrà illustrato un esempio di creazione di tre profili di crittografia denominati "CRES_HIGH", "CRES_MED" e "CRES_LOW".

1. Dall'interfaccia utente dell'ESA, selezionare **Security Services > Cisco IronPort Email Encryption**.
2. Fare clic su "Add Encryption Profile" (Aggiungi profilo di crittografia)."

3. Viene visualizzato il menu Profilo crittografia (Encryption Profile) ed è possibile assegnare al primo profilo di crittografia il nome "CRES_HIGH".
4. Selezionare "Protezione alta" per Protezione messaggi buste, se non è già selezionato.
5. Fare clic su **Invia** per salvare il profilo.



Ripetere quindi i passaggi da 2 a 5 per creare "CRES_MED" e "CRES_LOW". È sufficiente modificare il pulsante di opzione per la sicurezza dei messaggi per ogni profilo.

- Per il profilo CRES_HIGH, scegliere il pulsante di opzione "Protezione alta".
- Per il profilo CRES_MED, scegliere il pulsante di opzione "Protezione media".
- Per il profilo CRES_LOW, scegliere il pulsante di opzione "Nessuna password richiesta"

Si noterà che esistono opzioni per abilitare le conferme di lettura, abilitare le risposte sicure per tutti e abilitare l'inoltro sicuro dei messaggi. In Envelope Settings, facendo clic sul collegamento "Advanced" (Avanzate), è possibile selezionare uno dei tre algoritmi di crittografia simmetrica e specificare che la busta deve essere inviata senza l'applet di crittografia Java.

A destra di Envelope Settings, verrà visualizzato il collegamento ipertestuale "Messaggio di esempio". Facendo clic su questo pulsante, verrà visualizzato un esempio della busta messaggio protetto, ovvero ciò che il destinatario vedrà nel messaggio di posta elettronica dopo aver aperto l'allegato HTML.

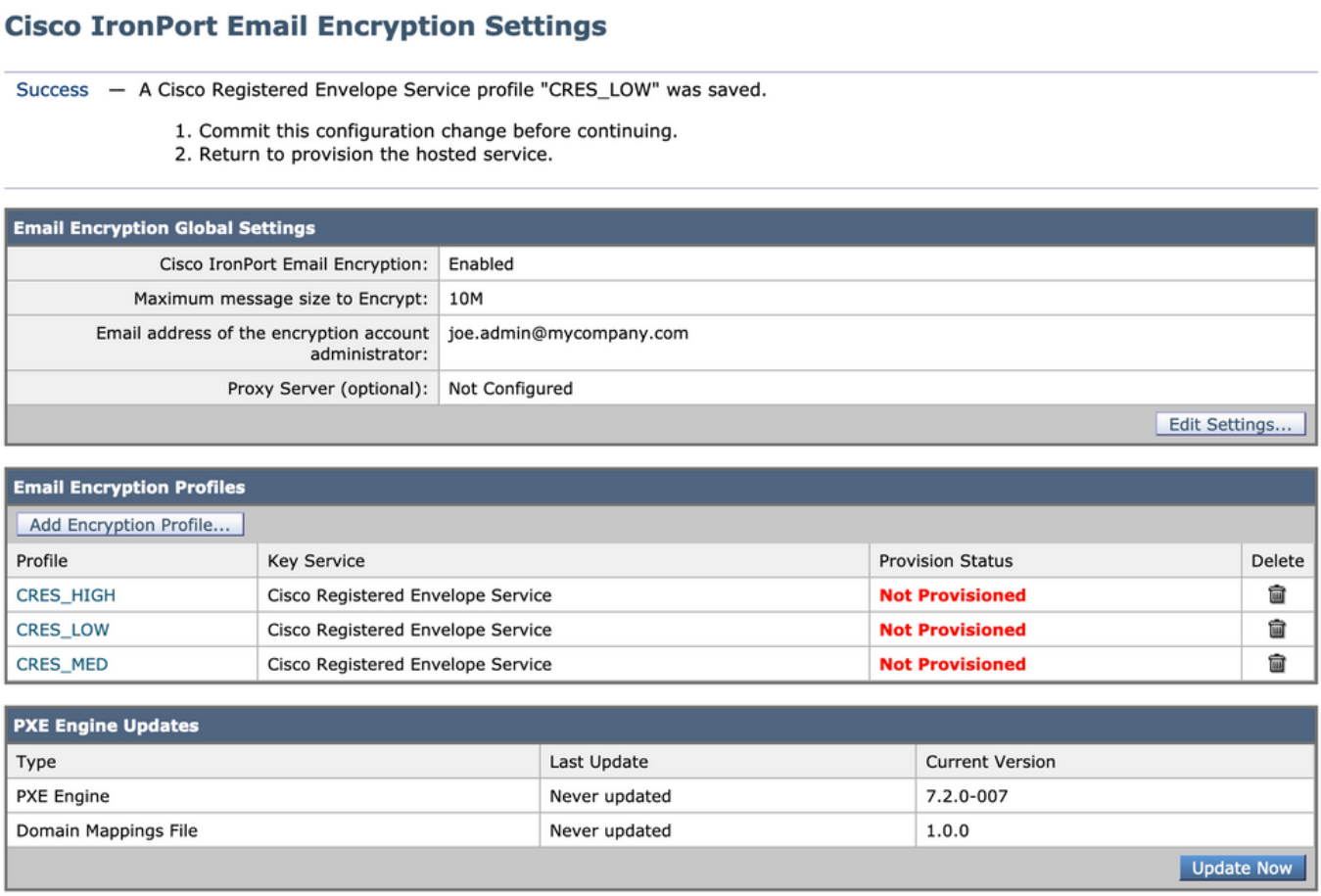
Conferme di lettura indica che il mittente del messaggio crittografato riceverà un messaggio di posta elettronica dal CRES quando il destinatario aprirà il messaggio protetto, ovvero quando il

destinatario avrà estratto la chiave simmetrica e decrittografato il messaggio.

A destra di Impostazioni messaggio verrà visualizzato il collegamento ipertestuale "Messaggio di esempio". Se si fa clic su questo pulsante, verrà visualizzato l'aspetto del messaggio aperto, ovvero quello che il destinatario vedrà dopo aver fornito le informazioni necessarie nella busta e aver aperto il messaggio crittografato.

Ricordarsi sempre di fare clic su **Invia** ed esegui commit delle modifiche.

Nella riga della tabella verrà visualizzato il pulsante "Provisioning". Il pulsante Provisioning non viene visualizzato fino a quando non si esegue il commit delle modifiche.



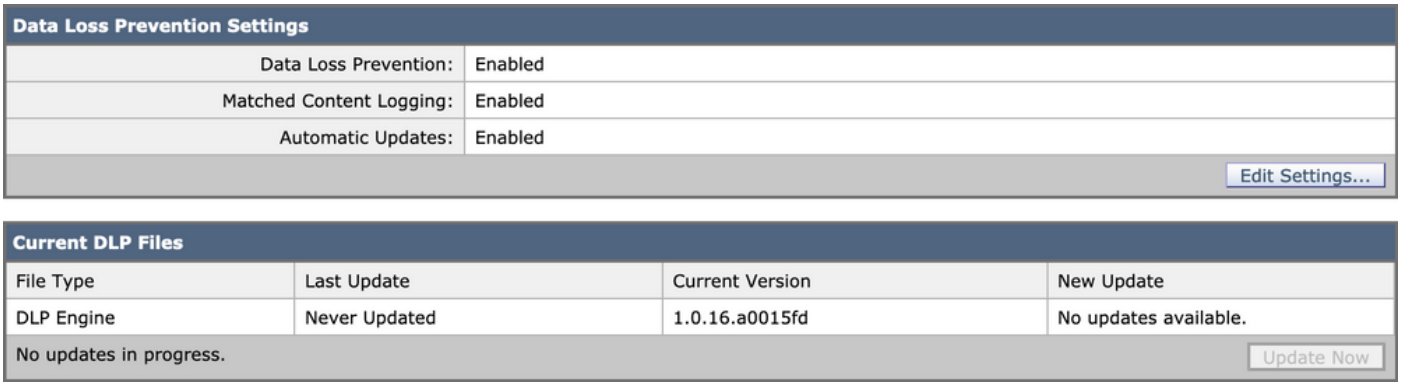
Fare nuovamente clic sul pulsante Provisioning. Questa operazione funzionerà solo dopo la creazione dell'account RES aziendale e l'aggiunta degli S/N dell'accessorio all'account. Se il conto RES è collegato al SEC, il processo di accantonamento avverrà in tempi relativamente brevi. In caso contrario, il processo dovrà prima essere completato.

Una volta completato il provisioning, la pagina Cisco IronPort Email Encryption mostrerà il profilo come sottoposto a provisioning.

4. Abilitazione della prevenzione della perdita dei dati

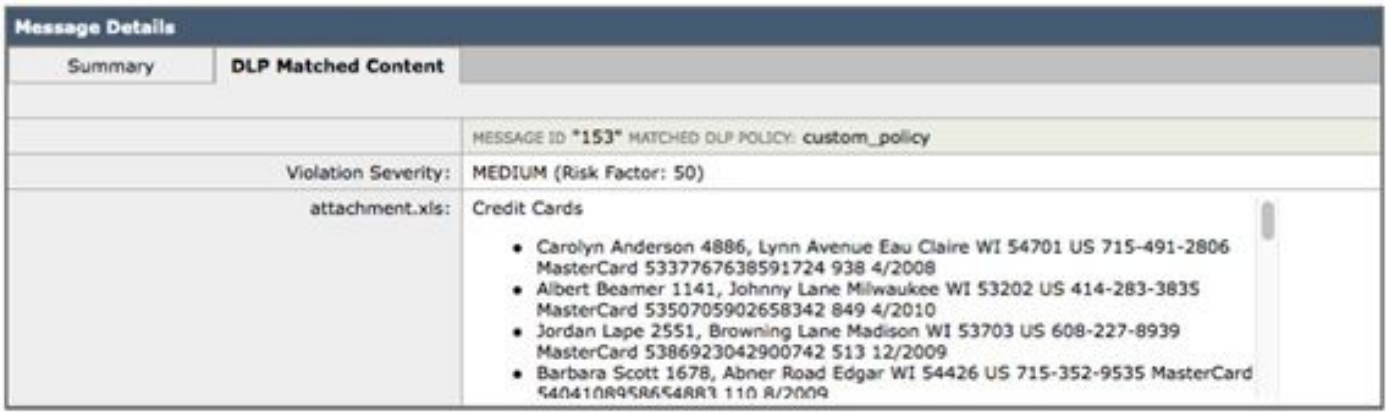
1. Dall'interfaccia utente ESA, selezionare **Security Services > Data Loss Prevention** (Servizi di sicurezza > Prevenzione della perdita di dati).
2. Fare clic su **Attiva...** per attivare DLP.
3. Accettare il Contratto di Licenza per la prevenzione della perdita dei dati.

4. Fare clic sulla casella di controllo Abilita registrazione contenuto corrispondente.
5. Selezionare la casella di controllo Attiva aggiornamenti automatici.
6. Fare clic su **Invia**.



Gli aggiornamenti per il motore di prevenzione della perdita dei dati e i classificatori di corrispondenza del contenuto predefiniti sull'accessorio sono indipendenti dagli aggiornamenti per altri servizi di sicurezza. Gli aggiornamenti regolari della firma Talos di 3-5 minuti sono diversi e non includono l'aggiornamento dei criteri di prevenzione della perdita dei dati e dei dizionari. È necessario abilitare gli aggiornamenti in questa posizione.

Quando "Registrazione contenuto corrispondente" è abilitato, consente a Gestione messaggi di mostrare il contenuto dell'e-mail che ha causato la violazione. Di seguito è riportato un esempio di verifica messaggi in cui viene mostrato il contenuto e-mail che ha causato la violazione della prevenzione della perdita dei dati. In questo modo, un amministratore può sapere esattamente quali dati hanno attivato uno specifico criterio di prevenzione della perdita dei dati.



Violazione della prevenzione della perdita dei dati

5. Creazione di azioni messaggio di prevenzione della perdita di dati

Crea quarantene DLP

Se desideri conservare una copia dei messaggi che violano i criteri di prevenzione della perdita dei dati, puoi creare singole quarantene per ogni tipo di violazione dei criteri. Ciò è particolarmente utile quando si esegue un POV "trasparente", in cui i messaggi in uscita che violano i criteri di prevenzione della perdita dei dati vengono registrati e recapitati, ma non viene eseguita alcuna azione sui messaggi.

1. Nell'SMA, selezionare **E-mail > Quarantena messaggi > Criterio, Virus ed epidemie in quarantena**
2. Ecco come dovrebbe apparire la tabella Quarantines prima di

iniziare:

Policy, Virus and Outbreak Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	N/A	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	23 Jul 2020 14:43 (GMT +00:00)	0	
Policy	Policy	0	Retain 10 days then Delete	N/A	0	
Unclassified	Unclassified	0	Retain 30 days then Release	N/A	0	
Virus	Antivirus	0	Retain 30 days then Delete	N/A	0	

Available space for Policy, Virus, Antimalware & Outbreak quarantines is 10G.

Messa in quarantena di virus ed epidemie

3. Fare clic sul pulsante "Aggiungi quarantena criteri" e creare una quarantena da utilizzare per i criteri di prevenzione della perdita dei dati.

Di seguito è riportato un esempio di quarantena eseguita per una violazione DLP media. La segmentazione delle quarantene è possibile e può essere richiesta per più regole di prevenzione della perdita dei dati:

Add Quarantine

Settings

Quarantine Name:	DLP Quarantine Violations
Retention Period:	14 Days
Default Action:	(•) Delete ( ) Release
	[x] Free up space by applying default action on messages upon space overflow Additional options to apply on Release action (when used for freeing up space) [ ] Modify Subject [ ] Add X-Header [ ] Strip Attachments
Local Users:	No users selected
Externally Authenticated Users:	No users selected
Custom User Roles:	No roles selected

Cancel | Submit

Esempio di quarantena DLP

Informazioni sulle azioni dei messaggi di prevenzione della perdita dei dati

Le azioni dei messaggi di prevenzione della perdita dei dati descrivono le azioni che l'ESA intraprenderà quando rileva una violazione di prevenzione della perdita dei dati in un messaggio e-mail in uscita. È possibile specificare le azioni DLP principali e secondarie e assegnare azioni diverse per tipi e severità di violazione diversi.

Le azioni principali includono:

- Consegna
- Drop
- Quarantena

Per uno stato di sola lettura in cui le violazioni dei criteri di prevenzione della perdita dei dati vengono registrate e segnalate ma i messaggi non vengono arrestati, messi in quarantena o crittografati, l'azione di recapito viene utilizzata con maggiore frequenza.

Le azioni secondarie includono:

- Invio di una copia in quarantena personalizzata o in quarantena ‘Policy’.
- **Crittografare il messaggio.** L'accessorio crittografa solo il corpo del messaggio. Le intestazioni dei messaggi non vengono crittografate.
- Modifica dell'intestazione Subject.
- Aggiunta di testo o codice HTML di esclusione di responsabilità al messaggio.
- Invio del messaggio a un mailhost di destinazione alternativo.
- Invio in copia in copia del messaggio.
- Invio della notifica di violazione del DLP al mittente e/o ad altri contatti.

Queste azioni non si escludono a vicenda: è possibile combinarne alcune in criteri di prevenzione della perdita dei dati diversi per esigenze di elaborazione diverse per gruppi di utenti diversi.

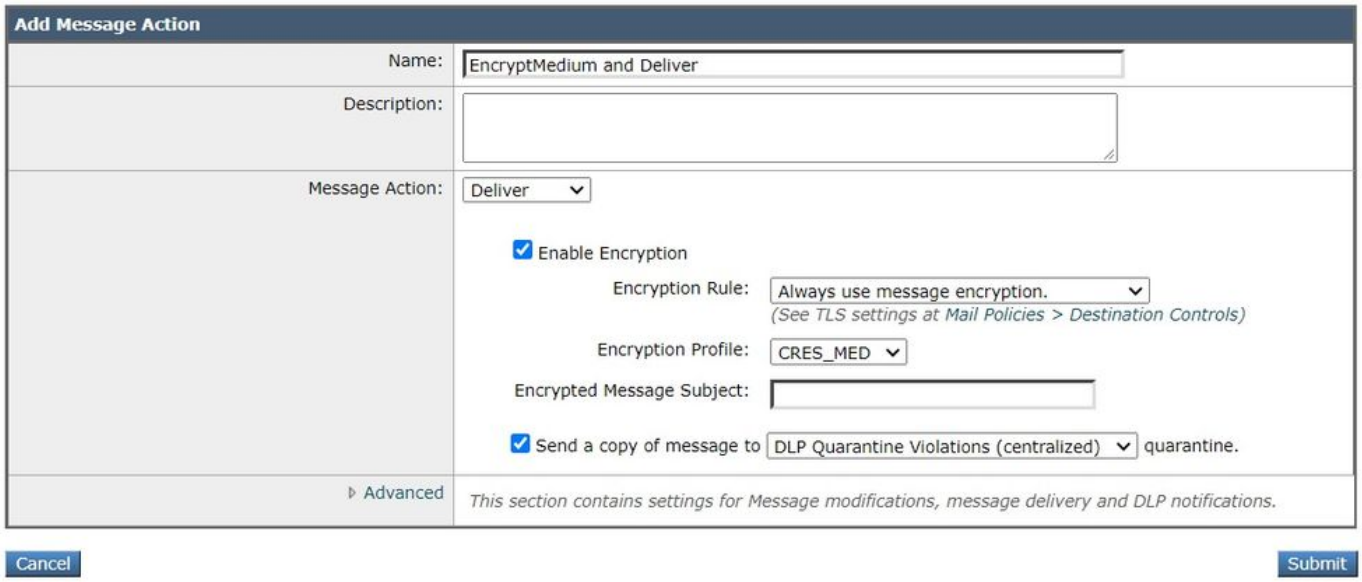
Implementeremo le seguenti azioni DLP: **Encrypt**

Queste azioni presuppongono che la crittografia sia concessa in licenza e configurata sull'ESA e che siano stati creati tre profili per la sicurezza alta, media e bassa, come è stato fatto nelle sezioni precedenti:

- CRES_ALTO
- CRES_MED
- CRES_LOW

Crea le azioni del messaggio di prevenzione della perdita dei dati

1. Vai a *Policy di posta > Personalizzazioni messaggi di prevenzione della perdita dei dati.*
2. Fare clic sul pulsante "Aggiungi azione messaggio" e aggiungere le seguenti azioni DLP. Assicurarsi di eseguire il commit della modifica dopo l'invio dell'azione messaggio



Azione messaggio

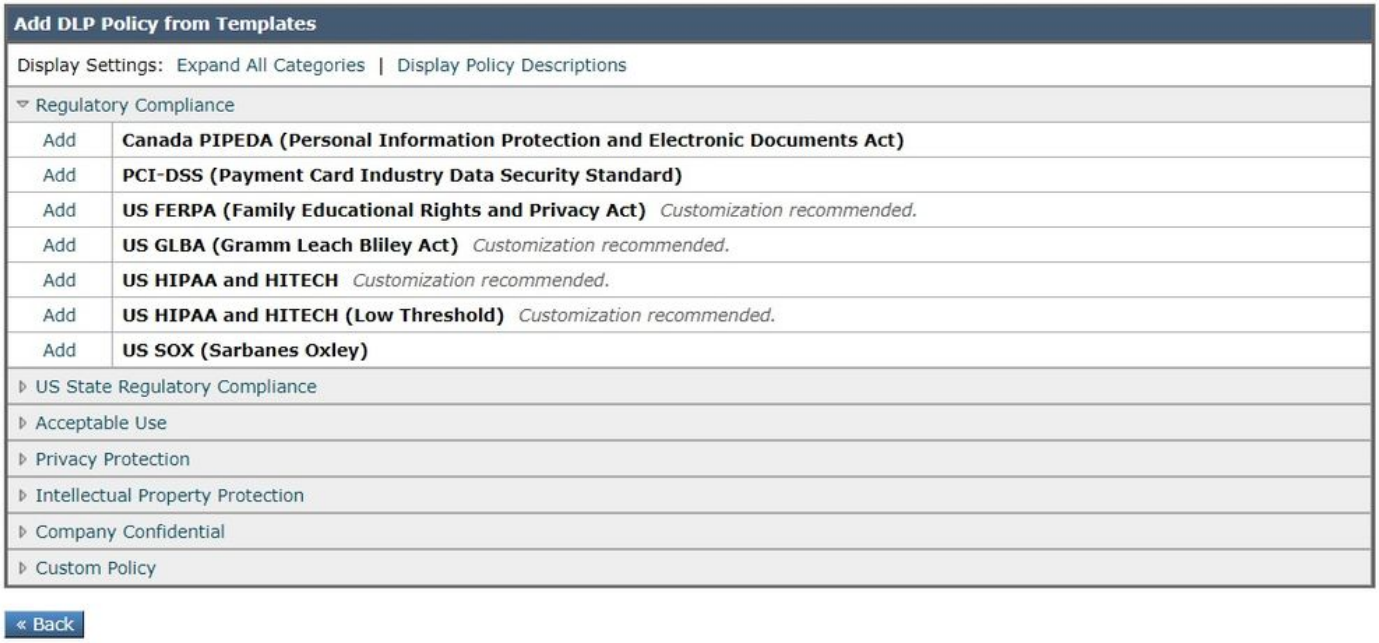
6. Creazione di politiche di prevenzione della perdita dei dati

I criteri di prevenzione della perdita dei dati includono:

- Insieme di condizioni che determinano se un messaggio in uscita contiene dati riservati
- Azioni da eseguire quando un messaggio contiene tali dati.

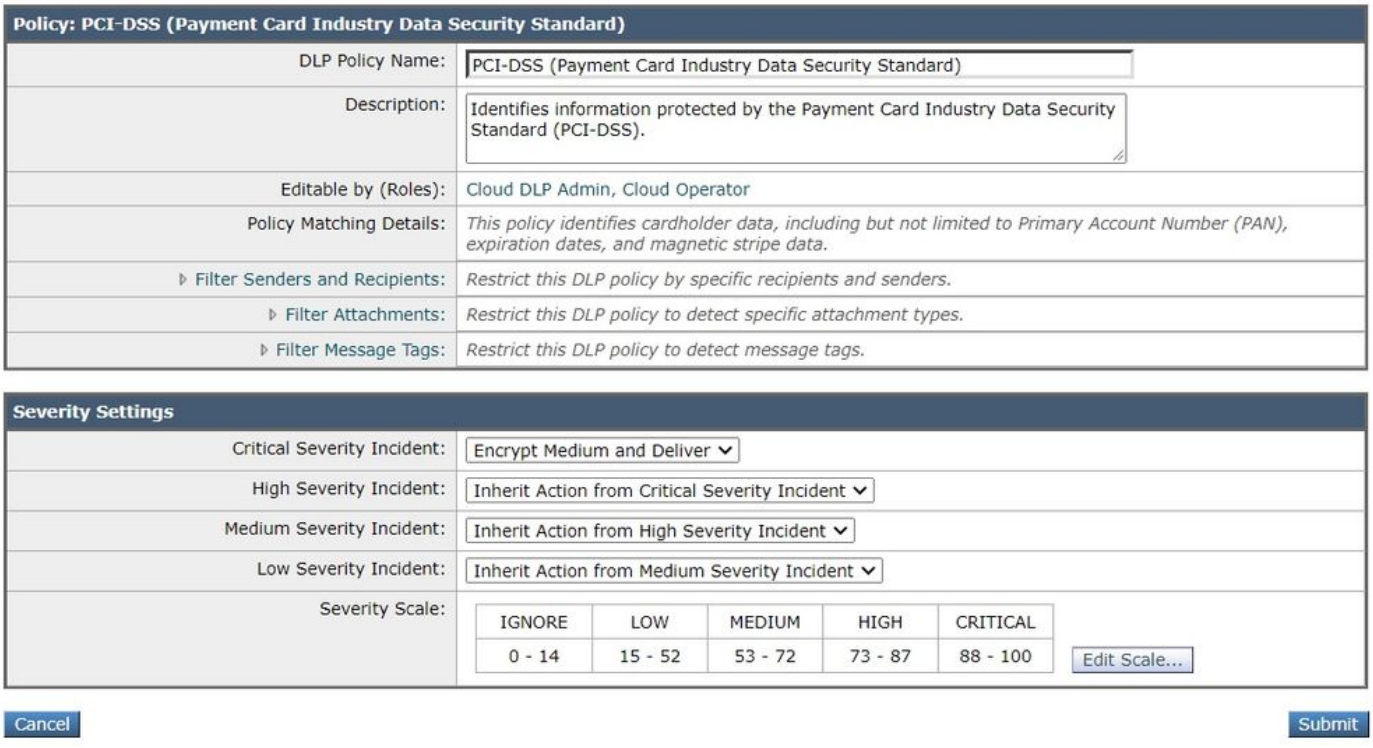
1. Passare a: *Mail Policies > DLP Policy Manager*

2. Fare clic su *'Aggiungi criteri di prevenzione della perdita dei dati'*
3. Apri il triangolo di divulgazione "Conformità alle normative".



Modello di criteri di prevenzione della perdita dei dati

4. Per la policy PCI, fare clic sul pulsante "Aggiungi" a sinistra di PCI-DSS.



Regola DLP di esempio PCI-DSS

5. Per l'incidente di gravità critica selezionare l'azione "Crittografa supporto e consegna" precedentemente configurata. Potremmo cambiare gli incidenti con livelli di gravità più bassi, ma per ora, facciamo in modo che ereditino i nostri incidenti con livelli di gravità critici. Inviare e confermare la modifica.

7. Applicazione dei criteri di prevenzione della perdita dei dati a un criterio e-mail in uscita

1. Accedere a: Criteri di posta > Criteri posta in uscita
2. Fare clic sulla cella di controllo relativa a DLP per il criterio predefinito. Se non è ancora stato abilitato, verrà visualizzato "Disabilitato".
3. Modificare il pulsante a discesa da Disabilita DLP ad Abilita DLP per visualizzare immediatamente i criteri di prevenzione della perdita dei dati appena creati.
4. Selezionare la casella di controllo "Attiva tutto". Inviare e quindi eseguire il commit delle modifiche.

Conclusioni

Per riassumere, abbiamo mostrato i passaggi necessari per preparare un'appliance Cisco Email Security all'invio di un'e-mail crittografata:

1. Abilitazione di Cisco IronPort Email Encryption
2. Registrazione delle ESA e dell'organizzazione con RES
3. Creazione di profili di crittografia
4. Abilitazione di DLP
5. Creazione di azioni messaggio DLP
6. Creazione di criteri di prevenzione della perdita dei dati
7. Applicazione dei criteri di prevenzione della perdita dei dati a un criterio e-mail in uscita

Ulteriori dettagli sono disponibili nella Guida per l'utente ESA corrispondente alla versione del software ESA. Le guide per l'utente sono disponibili al seguente collegamento:

http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html

Informazioni correlate

- Documentazione e supporto tecnico – Cisco Systems