

Guide des meilleures pratiques pour la prévention et le cryptage des pertes de données

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Guide des meilleures pratiques en matière de prévention de la perte de données et de cryptage](#)

[1. Activer le cryptage des e-mails Cisco IronPort sur les ESA](#)

[2. Enregistrez votre ou vos ESA\(s\) et votre organisation avec RES](#)

[3. Créer des profils de cryptage sur les ESA](#)

[4. Activation de la prévention des pertes de données \(DLP\)](#)

[5. Création d'actions de message de prévention de perte de données](#)

[6. Création de stratégies de prévention des pertes de données](#)

[7. Application de stratégies DLP à une stratégie de messagerie sortante](#)

[Conclusion](#)

[Informations connexes](#)

Introduction

Ce document décrit les meilleures pratiques en matière de prévention de perte de données (DLP) et de cryptage pour la sécurité de la messagerie Cisco.

Ce document traite de la configuration du cryptage des messages à l'aide de l'apppliance de sécurité de la messagerie Cisco (ESA) et du service cloud Cisco Registered Envelope Service (RES). Les clients peuvent utiliser le chiffrement des messages pour envoyer des messages individuels en toute sécurité sur Internet public, en utilisant différents types de politiques, notamment le filtrage de contenu et la DLP. La création de ces politiques sera examinée dans d'autres documents de cette série. Ce document se concentre sur la préparation de l'ESA à envoyer du courrier chiffré afin que les politiques puissent utiliser le chiffrement comme une action.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Ce document décrit les étapes suivantes :

1. Activation du cryptage des e-mails Cisco IronPort
2. Enregistrez votre ou vos ESA(s) et votre organisation avec RES
3. Création de profils de chiffrement
4. Activation de DLP
5. Création d'actions de message DLP
6. Création de stratégies DLP
7. Application de stratégies DLP à une stratégie de messagerie sortante

Une fois ces étapes effectuées, l'administrateur ESA peut créer avec succès une stratégie qui utilisera le chiffrement comme action.

Le chiffrement de messagerie électronique Cisco IronPort est également appelé chiffrement RES. RES est le nom que nous utilisons pour les " principaux serveurs " dans le cloud Cisco. La solution de chiffrement RES utilise le chiffrement à clé symétrique, ce qui signifie que la clé utilisée pour chiffrer le message est la même clé utilisée pour déchiffrer le message. Chaque message chiffré utilise une clé unique, qui permet à l'expéditeur d'avoir un contrôle granulaire sur un message après son envoi (par exemple, pour le verrouiller ou l'expirer afin que le destinataire ne puisse plus l'ouvrir), sans affecter aucun autre message. Lors du chiffrement d'un message, l'ESA stocke la clé de chiffrement et les métadonnées dans CRES sur chaque message chiffré.

L'ESA peut décider de chiffrer un message de différentes manières : via " indicateur " (comme le contenu d'objet), via la correspondance de filtre de contenu ou via la politique DLP, par exemple. Une fois que l'ESA a décidé de chiffrer un message, elle le fait avec un " de profil de chiffrement " spécifié créé dans " Security Services > Cisco IronPort Email Encryption " — la table nommée " Email Encryption Profiles ". Par défaut, il n'existe aucun profil de chiffrement. Cette question sera abordée dans le *paragraphe 3. Création de profils de chiffrement*.

Guide des meilleures pratiques en matière de prévention de la perte de données et de cryptage

1. Activer le cryptage des e-mails Cisco IronPort sur les ESA

Note: Si vous avez plusieurs ESA dans un cluster, l'étape n°1 ne doit être exécutée qu'une seule fois, car ces paramètres sont généralement gérés au niveau du cluster. Si vous avez plusieurs machines qui ne sont pas en cluster ou si vous gérez ces paramètres au niveau de la machine, l'étape n° 1 doit être exécutée sur chaque ESA.

1. À partir de l'interface utilisateur ESA, accédez à **Security Services > Cisco IronPort Email Encryption**.
2. Cochez cette case pour activer le cryptage des e-mails Cisco IronPort.
3. Acceptez le Contrat de licence de l'utilisateur final (CLUF), Contrat de licence de chiffrement

du courrier électronique Cisco IronPort.

4. Dans les *paramètres globaux de chiffrement des e-mails*, cliquez sur **Modifier les paramètres...** Spécifiez l'adresse e-mail de l'administrateur/de la personne qui est l'administrateur RES principal pour le compte. Ce compte de messagerie sera associé à l'administration de l'environnement RES pour la société. Facultatif: La taille maximale par défaut du message à chiffrer est de 10 millions. Vous pouvez augmenter/diminuer la taille à ce moment-là si vous le souhaitez. Facultatif: Si vous avez un proxy que le ESA devra passer pour se connecter à RES via HTTPS, ajoutez les paramètres de proxy et d'authentification nécessaires pour lui permettre de passer par le proxy.
5. Envoyez et confirmez vos modifications de configuration.

À ce stade, vous devriez voir les paramètres globaux " de chiffrement des e-mails " définis sur quelque chose comme ceci, mais sans profils répertoriés pour le moment :

Cisco IronPort Email Encryption Settings

Success — Settings have been saved.

Email Encryption Global Settings	
Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	joe.admin@mycompany.com
Proxy Server (optional):	Not Configured

[Edit Settings...](#)

Email Encryption Profiles	
Add Encryption Profile...	
No Encryption Profiles Configured.	

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	Never updated	7.2.0-007
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

2. Enregistrez votre ou vos ESA(s) et votre organisation avec RES

L'étape 2 prend principalement part à l'extérieur de la console d'administration ESA.

Note: Les informations relatives à l'enregistrement de l'ESA sont également disponibles dans TechNote : [Cisco RES : Exemple de configuration du provisionnement de compte pour le ESA virtuel, hébergé et matériel](#)

Veuillez envoyer un courriel directement à RES : stg-cres-provisioning@cisco.com.

Afin de provisionner un compte CRES pour vos profils de cryptage ESA, veuillez nous fournir les informations suivantes :

1. Nom du compte (**Veuillez indiquer le nom exact de la société, car vous devez l'indiquer.**)
Pour les comptes clients hébergés/de sécurité de la messagerie en nuage (CES), notez le

- nom de votre compte pour terminer par "<Nom du compte> HÉBERGÉ »
2. Adresse(s) e-mail à utiliser pour l'administrateur du compte (**veuillez spécifier l'adresse e-mail d'administrateur correspondante**)
 3. Numéro(s) de série complet de l'appareil Un numéro de série de l'appareil peut être localisé à partir de l'interface utilisateur graphique de l'ESA (Administration du système > Clés de fonction) ou de l'interface de ligne de commande de l'ESA via la commande « version ». La fourniture d'une licence de numéro de licence virtuel (VLN) ou de clé d'activation de produit (PAK) n'est pas acceptable, car un numéro de série complet de l'appareil est requis pour l'administration des comptes CRES.
 4. Noms de domaine qui doivent être mappés au compte CRES à des fins d'administration

Note: Si vous avez déjà un compte CRES, veuillez indiquer le nom de la société ou le numéro de compte CRES existant. Cela garantit que les nouveaux numéros de série de l'appareil sont ajoutés au compte approprié et évite toute duplication des informations de l'entreprise et du provisionnement.

Soyez assuré que si vous envoyez un e-mail concernant l'approvisionnement d'un compte CRES, nous vous répondrons par un (1) jour ouvrable. Si vous avez besoin d'une assistance et d'une assistance immédiates, envoyez une demande d'assistance au TAC Cisco. Vous pouvez le faire par l'intermédiaire de Support Case Manager (<https://mycase.cloudapps.cisco.com/case>) ou par téléphone (<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>).

Note: Une fois cette demande envoyée par e-mail, il peut s'écouler un jour avant que votre compte RES de société soit créé (s'il n'a pas encore été créé) et que les S/Ns soient ajoutés. La tâche " approvisionnement ", à l'étape 3, ne fonctionnera pas tant que ce n'est pas terminé.

3. Créer des profils de cryptage sur les ESA

Note: Si vous avez plusieurs ESA dans un cluster, l'étape n°1 ne doit être exécutée qu'une seule fois, car ces paramètres sont généralement gérés au niveau du cluster. Si vous avez plusieurs machines qui ne sont pas en cluster ou si vous gérez ces paramètres au niveau de la machine, l'étape n° 1 doit être exécutée sur chaque ESA.

Un profil de cryptage indique comment envoyer les messages chiffrés. Par exemple, une entreprise peut avoir besoin d'envoyer des enveloppes haute sécurité pour un segment de ses destinataires, par exemple ceux auxquels elle sait qu'elle enverra fréquemment des données hautement sensibles. La même organisation peut avoir d'autres segments de sa communauté de destinataires qui reçoivent des informations moins sensibles et qui sont peut-être moins patients à avoir à fournir un ID utilisateur et un mot de passe pour recevoir du courrier chiffré. Ces destinataires seraient de bons candidats pour un type d'enveloppe de faible sécurité. Le fait d'avoir plusieurs profils de cryptage permet à l'entreprise d'adapter le format de message chiffré au public. D'un autre côté, de nombreuses entreprises peuvent se passer d'un seul profil de cryptage.

Pour ce document, nous allons montrer un exemple de création de trois profils de chiffrement nommés " CRES_HIGH ", " CRES_MED " et " CRES_LOW ".

1. À partir de l'interface utilisateur ESA, accédez à **Security Services > Cisco IronPort Email**

Encryption.

2. Cliquez sur “Ajouter un profil de chiffrement...”
3. Le menu Profil de chiffrement s'ouvre et vous pouvez nommer votre premier profil de chiffrement “CRES_HIGH”.
4. Sélectionnez « Haute sécurité » pour la sécurité des messages de l'enveloppe, si ce n'est déjà fait.
5. Cliquez sur **Soumettre** pour enregistrer ce profil.

Encryption Profile Settings	
Profile Name:	<input type="text" value="CRES_HIGH"/>
Key Server Settings	
Key Service Type:	<input type="text" value="Cisco Registered Envelope Service"/>
Proxy:	<i>A proxy server is not currently configured.</i>
Cisco Registered Envelope Service URL:	<input type="text" value="https://res.cisco.com"/>
Advanced	<i>Advanced key server settings</i>
Envelope Settings	
Envelope Message Security:	<input checked="" type="radio"/> High Security <i>Recipient must enter a passphrase to open the encrypted message, even if credentials are cached ("Remember Me" selected).</i> <input type="radio"/> Medium Security <i>No passphrase entry required if recipient credentials are cached ("Remember Me" selected).</i> <input type="radio"/> No Passphrase Required <i>The recipient does not need a passphrase to open the encrypted message.</i>
Logo Link:	<input checked="" type="radio"/> No link <input type="radio"/> Custom link URL: <input type="text"/> <i>By defining a URL, the logo in the upper left corner of the recipient envelope will become a link (example: http://www.mycompany.com/).</i>
Read Receipts:	<input checked="" type="checkbox"/> Enable Read Receipts
Advanced	<i>Advanced envelope settings</i>
Example Envelope	
Message Settings	
End-User Controls:	<input type="checkbox"/> Enable Secure Reply All <input type="checkbox"/> Enable Secure Message Forwarding
Example Message	
Notification Settings	
Localized Envelopes:	<input type="checkbox"/> Use Localized Envelope
Encrypted Message HTML Notification:	System Generated Preview Message <i>(see Mail Policies > Text Resources > Encryption Notification Template - HTML)</i>
Encrypted Message Text Notification:	System Generated Preview Message <i>(see Mail Policies > Text Resources > Encryption Notification Template - Text)</i>
Encryption Failure Notification:	Message Subject: <input type="text" value="[ENCRYPTION FAILURE]"/> Message Body: System Generated Preview Message <i>(see Mail Policies > Text Resources > DSN Bounce and Encryption Failure Notification Template)</i>
File name of the envelope attached to the encryption notification:	<input type="text" value="securedoc_\${date}T\${time}.html"/>

Ensuite, répétez les étapes 2 à 5 pour créer « CRES_MED » et « CRES_LOW » — il vous suffit de modifier la case d'option pour la sécurité des messages de l'enveloppe pour chaque profil.

- Pour le profil CRES_HIGH, sélectionnez la case d'option “ High Security ”.
- Pour le profil CRES_MED, sélectionnez la case d'option “ Medium Security ”.
- Pour le profil CRES_LOW, sélectionnez la case d'option “ Aucun mot de passe requis ”

Vous remarquerez qu'il existe des options permettant d'activer les accusés de réception en lecture, d'activer la réponse sécurisée tout et d'activer le transfert sécurisé des messages. Dans Paramètres de l'enveloppe, si vous cliquez sur le lien “ Avancé ”, vous pouvez sélectionner l'un des trois algorithmes de chiffrement symétrique et spécifier que l'enveloppe est envoyée sans l'applet de chiffrement Java.

À droite de Paramètres de l'enveloppe, le lien “ Exemple de message ” hypertexte s'affiche. Si vous cliquez sur cette option, vous obtiendrez un exemple de message sécurisé — ce que le destinataire verra dans son e-mail après avoir ouvert la pièce jointe HTML.

Lire les accusés de réception signifie que l'expéditeur du message chiffré recevra un e-mail de CRES lorsque le destinataire ouvrira le message sécurisé (c'est-à-dire que le destinataire a retiré la clé symétrique et déchiffré le message).

À droite des paramètres du message, le lien hypertexte Exemple de message s'affiche. Si vous cliquez sur cette option, vous verrez à quoi ressemblera le message ouvert — ce que le destinataire verra une fois qu'il aura fourni les informations nécessaires dans l'enveloppe et qu'il aura ouvert le message chiffré.

N'oubliez pas de cliquer sur **Soumettre** et valider les modifications.

La ligne du tableau affiche ensuite un bouton ” de provisionnement “. Le bouton Provisionnement n'apparaît qu'après validation des modifications.

Cisco IronPort Email Encryption Settings

Success — A Cisco Registered Envelope Service profile "CRES_LOW" was saved.

1. Commit this configuration change before continuing.
2. Return to provision the hosted service.

Email Encryption Global Settings	
Cisco IronPort Email Encryption:	Enabled
Maximum message size to Encrypt:	10M
Email address of the encryption account administrator:	joe.admin@mycompany.com
Proxy Server (optional):	Not Configured

[Edit Settings...](#)

Email Encryption Profiles			
Add Encryption Profile...			
Profile	Key Service	Provision Status	Delete
CRES_HIGH	Cisco Registered Envelope Service	Not Provisioned	
CRES_LOW	Cisco Registered Envelope Service	Not Provisioned	
CRES_MED	Cisco Registered Envelope Service	Not Provisioned	

PXE Engine Updates		
Type	Last Update	Current Version
PXE Engine	Never updated	7.2.0-007
Domain Mappings File	Never updated	1.0.0

[Update Now](#)

Cliquez à nouveau sur le bouton Provisionner, cela ne fonctionnera qu'après la création du compte RES de votre société et l'ajout des S/N de l'appliance à votre compte. Si le compte RES est lié à l'ESA, le processus d'approvisionnement se déroulera relativement rapidement. Si ce n'est pas le cas, ce processus devra d'abord se terminer.

Une fois le provisionnement terminé, votre page de chiffrement des e-mails Cisco IronPort affiche le profil tel qu'il est configuré.

4. Activation de la prévention des pertes de données (DLP)

1. À partir de l'interface utilisateur ESA, accédez à **Services de sécurité > Prévention de perte de données**.

2. Cliquez sur **Activer...** pour activer DLP.
3. Acceptez le contrat de licence EULA, Data Loss Prevention.
4. Cochez la case Activer la journalisation du contenu correspondant.
5. Cochez la case Activer les mises à jour automatiques.
6. Cliquez sur Submit.

Data Loss Prevention Settings	
Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Automatic Updates:	Enabled

[Edit Settings...](#)

Current DLP Files			
File Type	Last Update	Current Version	New Update
DLP Engine	Never Updated	1.0.16.a0015fd	No updates available.

No updates in progress. [Update Now](#)

Les mises à jour pour le moteur DLP et les classificateurs de correspondance de contenu prédéfinis sur votre appareil sont indépendantes des mises à jour pour d'autres services de sécurité. Les mises à jour de signature Talos régulières de 3 à 5 minutes sont différentes et n'incluent pas la mise à jour des politiques et des dictionnaires DLP. Les mises à jour doivent être activées ici.

Lorsque "" de journalisation du contenu mappé est activée, elle permet au suivi des messages d'afficher le contenu de l'e-mail qui a causé la violation. Voici un exemple de suivi des messages qui montre le contenu de l'e-mail à l'origine de la violation DLP. De cette manière, un administrateur peut savoir exactement quelles données ont déclenché une stratégie DLP spécifique.

Message Details	
Summary	DLP Matched Content
	MESSAGE ID *153* MATCHED DLP POLICY: custom_policy
Violation Severity:	MEDIUM (Risk Factor: 50)
attachment.xls:	Credit Cards <ul style="list-style-type: none"> • Carolyn Anderson 4886, Lynn Avenue Eau Claire WI 54701 US 715-491-2806 MasterCard 5337767638591724 938 4/2008 • Albert Beamer 1141, Johnny Lane Milwaukee WI 53202 US 414-283-3835 MasterCard 5350705902658342 849 4/2010 • Jordan Lape 2551, Browning Lane Madison WI 53703 US 608-227-8939 MasterCard 5386923042900742 513 12/2009 • Barbara Scott 1678, Abner Road Edgar WI 54426 US 715-352-9535 MasterCard 540410R95R654RR7 110 R/2009

Violation de la prévention des pertes de données

5. Création d'actions de message de prévention de perte de données

Créer des quarantaines DLP

Si vous souhaitez conserver une copie des messages qui violent les stratégies DLP, vous pouvez créer des quarantaines de stratégie individuelles pour chaque type de violation de stratégie. Ceci est particulièrement utile lors de l'exécution d'un PDV transparent, où les messages sortants violant les stratégies DLP sont consignés et remis mais aucune action n'est entreprise sur les messages.

1. Sur SMA, accédez à **Email > Message Quarantine > Policy, Virus and Outbreak**

Quarantines.

2. Voici à quoi devrait ressembler le tableau Quarantines avant de commencer

:

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.

Quarantaine des attaques et des virus de stratégie

3. Cliquez sur le bouton “Ajouter une” de quarantaine de stratégie et créez une quarantaine à utiliser par les stratégies DLP.

Voici un exemple de quarantaine effectuée pour une violation DLP moyenne. La segmentation des quarantaines est possible et peut être souhaitée pour plusieurs règles DLP :

Add Quarantine

Settings	
Quarantine Name:	<input type="text" value="DLP Quarantine Violations"/>
Retention Period:	<input type="text" value="14"/> Days <input type="button" value="v"/>
Default Action:	<input checked="" type="radio"/> Delete <input type="radio"/> Release
	<input checked="" type="checkbox"/> 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)
	<input type="checkbox"/> Modify Subject <input type="checkbox"/> Add X-Header <input type="checkbox"/> Strip Attachments
Local Users:	No users selected
Externally Authenticated Users:	No users selected
Custom User Roles:	No roles selected

Exemple de quarantaine DLP

À propos des actions de message DLP

Les actions de message DLP décrivent les actions que l'ESA va entreprendre lorsqu'il détecte une violation DLP dans un e-mail sortant. Vous pouvez spécifier des actions DLP principales et secondaires et différentes actions peuvent être affectées pour différents types de violation et de gravité.

Les principales actions sont les suivantes :

- Offrir
- Déposer
- Quarantaine

Dans un état en lecture seule où les violations DLP sont consignées et signalées mais où les messages ne sont pas arrêtés/mis en quarantaine ou chiffrés, l'action de livraison est le plus souvent utilisée.

Les actions secondaires incluent :

- Envoi d'une copie à une quarantaine personnalisée ou à une quarantaine de stratégie.
- **Chiffrez le message.** L'appliance chiffre uniquement le corps du message. Il ne chiffre pas les en-têtes de message.
- Modification de l'en-tête Objet.
- Ajout de texte/HTML d'exclusion de responsabilité au message.
- Envoi du message à un autre hôte de messagerie de destination.
- Envoi de copies Cci du message.
- Envoi d'une notification de violation DLP à l'expéditeur et/ou à d'autres contacts.

Ces actions ne s'excluent pas mutuellement : vous pouvez en combiner certaines dans différentes stratégies DLP pour différents besoins de traitement pour différents groupes d'utilisateurs.

Nous allons mettre en oeuvre les actions DLP suivantes : **Chiffrement**

Ces actions supposent que le chiffrement est sous licence et configuré sur le SEEE et que trois profils ont été créés pour la sécurité élevée, moyenne et faible, comme cela a été fait dans les sections précédentes :

- CRES_ÉLEVÉ
- CRES_MED
- CRES_LOW

Créer des actions de message DLP

1. Accédez à *Politiques de messagerie > Personnalisations des messages DLP*.
2. Cliquez sur le bouton "Ajouter un" d'action de message et ajoutez les actions DLP suivantes. Veillez à valider la modification après avoir envoyé votre action de message

Add Message Action

Name: EncryptMedium and Deliver

Description:

Message Action: Deliver

Enable Encryption

Encryption Rule: Always use message encryption. (See TLS settings at Mail Policies > Destination Controls)

Encryption Profile: CRES_MED

Encrypted Message Subject:

Send a copy of message to DLP Quarantine Violations (centralized) quarantine.

Advanced This section contains settings for Message modifications, message delivery and DLP notifications.

Cancel

Submit

Action de message

6. Création de stratégies de prévention des pertes de données

Une stratégie DLP inclut :

- Ensemble de conditions déterminant si un message sortant contient des données sensibles
- Les actions à entreprendre lorsqu'un message contient de telles données.

1. Accédez à : *Politiques de messagerie > Gestionnaire de stratégies DLP*
2. Cliquez sur *Ajouter une stratégie DLP*
3. Ouvrez le triangle “ Conformité réglementaire ” divulgation.

Add DLP Policy from Templates	
Display Settings: Expand All Categories Display Policy Descriptions	
▼ Regulatory Compliance	
Add	Canada PIPEDA (Personal Information Protection and Electronic Documents Act)
Add	PCI-DSS (Payment Card Industry Data Security Standard)
Add	US FERPA (Family Educational Rights and Privacy Act) <i>Customization recommended.</i>
Add	US GLBA (Gramm Leach Bliley Act) <i>Customization recommended.</i>
Add	US HIPAA and HITECH <i>Customization recommended.</i>
Add	US HIPAA and HITECH (Low Threshold) <i>Customization recommended.</i>
Add	US SOX (Sarbanes Oxley)
▶ US State Regulatory Compliance	
▶ Acceptable Use	
▶ Privacy Protection	
▶ Intellectual Property Protection	
▶ Company Confidential	
▶ Custom Policy	

[« Back](#)

Modèle de stratégie DLP

4. Pour la stratégie PCI, cliquez sur le bouton Ajouter à gauche de PCI-DSS.

Policy: PCI-DSS (Payment Card Industry Data Security Standard)	
DLP Policy Name:	PCI-DSS (Payment Card Industry Data Security Standard)
Description:	Identifies information protected by the Payment Card Industry Data Security Standard (PCI-DSS).
Editable by (Roles):	Cloud DLP Admin, Cloud Operator
Policy Matching Details:	<i>This policy identifies cardholder data, including but not limited to Primary Account Number (PAN), expiration dates, and magnetic stripe data.</i>
▶ Filter Senders and Recipients:	<i>Restrict this DLP policy by specific recipients and senders.</i>
▶ Filter Attachments:	<i>Restrict this DLP policy to detect specific attachment types.</i>
▶ Filter Message Tags:	<i>Restrict this DLP policy to detect message tags.</i>

Severity Settings											
Critical Severity Incident:	Encrypt Medium and Deliver ▼										
High Severity Incident:	Inherit Action from Critical Severity Incident ▼										
Medium Severity Incident:	Inherit Action from High Severity Incident ▼										
Low Severity Incident:	Inherit Action from Medium Severity Incident ▼										
Severity Scale:	<table border="1"> <thead> <tr> <th>IGNORE</th> <th>LOW</th> <th>MEDIUM</th> <th>HIGH</th> <th>CRITICAL</th> </tr> </thead> <tbody> <tr> <td>0 - 14</td> <td>15 - 52</td> <td>53 - 72</td> <td>73 - 87</td> <td>88 - 100</td> </tr> </tbody> </table> Edit Scale...	IGNORE	LOW	MEDIUM	HIGH	CRITICAL	0 - 14	15 - 52	53 - 72	73 - 87	88 - 100
IGNORE	LOW	MEDIUM	HIGH	CRITICAL							
0 - 14	15 - 52	53 - 72	73 - 87	88 - 100							

[Cancel](#)

[Submit](#)

Exemple de règle DLP PCI-DSS

5. Pour l'incident de gravité critique, sélectionnez l'action « Chiffrer le support et livrer » que nous avons précédemment configurée. Nous pourrions changer les incidents de gravité inférieure mais pour l'instant, laissons-les hériter de notre incident de gravité critique. Envoyez et validez la modification.

7. Application de stratégies DLP à une stratégie de messagerie sortante

1. Accédez à : Politiques de messagerie > Politiques de messagerie sortante
2. Cliquez sur la cellule de contrôle de DLP pour la stratégie par défaut. Il lit “ Désactivé ” si vous ne l'avez pas encore activé.
3. Modifiez le bouton de menu déroulant Disable DLP (Désactiver DLP) en Enable DLP (Activer DLP) et vous recevrez immédiatement la stratégie DLP que vous venez de créer.
4. Cochez la case “ Activer tout ”. Envoyez et confirmez les modifications.

Conclusion

En résumé, nous avons présenté les étapes nécessaires pour préparer un dispositif de sécurité de la messagerie Cisco à envoyer un e-mail chiffré :

1. Activation du cryptage des e-mails Cisco IronPort
2. Enregistrez votre ou vos ESA(s) et votre organisation avec RES
3. Création de profils de chiffrement
4. Activation de DLP
5. Création d'actions de message DLP
6. Création de stratégies DLP
7. Application de stratégies DLP à une stratégie de messagerie sortante

Des informations supplémentaires sont disponibles dans le guide de l'utilisateur ESA correspondant à votre version du logiciel ESA. Les guides d'utilisation sont disponibles à l'adresse suivante :

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

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)