

Best Practices Guide for Data Loss Prevention and Encryption (Handleiding voor best practices voor preventie en versleuteling van gegevensverlies)

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Best Practice Guide for Data Loss Prevention and Encryption Best Practices](#)

[1. E-mailcodering via Cisco IronPort inschakelen op de ESA\(s\)](#)

[2. Registreer uw ESA\(s\) en uw organisatie bij RES](#)

[3. Coderingsprofielen op de ESA\(s\) aanmaken](#)

[4. Preventie van gegevensverlies \(DLP\) inschakelen](#)

[5. Berichtacties voor het voorkomen van gegevensverlies maken](#)

[6. Beleidsregels voor het voorkomen van gegevensverlies opstellen](#)

[7. DLP-beleid toepassen op een uitgaand e-mailbeleid](#)

[Conclusie](#)

[Gerelateerde informatie](#)

Inleiding

In dit document worden de best practices voor DLP (Data Loss Prevention) en codering voor Cisco Email Security beschreven.

In dit document wordt de configuratie van berichtencodering besproken met behulp van de Cisco Email Security Appliance (ESA) en de cloudgebaseerde Cisco Registered Envelope Service (RES). Klanten kunnen berichtencodering gebruiken om afzonderlijke berichten veilig over het openbare internet te verzenden, met behulp van verschillende soorten beleid, waaronder contentfiltering en DLP. De creatie van dit beleid wordt besproken in andere documenten binnen deze reeks. Dit document richt zich op het voorbereiden van de ESA op het versturen van versleutelde post, zodat het beleid versleuteling als een actie kan gebruiken.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

In dit document worden de volgende stappen besproken:

1. E-mailcodering van Cisco IronPort inschakelen
2. Registreer uw ESA(s) en uw organisatie bij RES
3. Coderingsprofielen maken
4. DLP inschakelen
5. DLP-berichtacties maken
6. DLP-beleid maken
7. DLP-beleid toepassen op een uitgaand e-mailbeleid

Zodra deze stappen met succes zijn voltooid, kan de ESA-beheerder met succes een beleid maken dat versleuteling als een actie gebruikt.

Cisco IronPort Email Encryption wordt ook wel RES Encryption genoemd. RES is de naam die we gebruiken voor de "key servers" in de Cisco Cloud. De RES-coderingsoplossing maakt gebruik van symmetrische sleutelcodering - wat betekent dat de sleutel die wordt gebruikt om het bericht te coderen dezelfde sleutel is die wordt gebruikt om het bericht te decoderen. Elk gecodeerd bericht gebruikt een unieke sleutel, waarmee de afzender granulaire controle over een bericht kan hebben nadat het is verzonden - bijvoorbeeld om het te vergrendelen of te verlopen, zodat de ontvanger het niet langer kan openen - zonder andere berichten te beïnvloeden. Bij het versleutelen van een bericht slaat de ESA de coderingssleutel en metagegevens op in CRES over elk versleuteld bericht.

De ESA kan besluiten om een bericht op vele manieren te versleutelen - via "flag" (zoals onderwerpinhoud), via Content Filter matching, of via DLP-beleid, bijvoorbeeld. Zodra de ESA besluit om een bericht te versleutelen, doet het dit met een opgegeven "Encryptieprofiel" gemaakt in "Security Services > Cisco IronPort Email Encryption" - de tabel met de naam "E-mailversleutelingsprofielen". Er zijn standaard geen coderingsprofielen. Dit zal in 3 besproken worden. Coderingsprofielen maken.

Best Practice Guide for Data Loss Prevention and Encryption Best Practices

1. E-mailcodering via Cisco IronPort inschakelen op de ESA(s)

 **Opmerking:** als u meerdere ESA's in een cluster hebt, hoeft stap #1 slechts eenmaal te worden uitgevoerd, omdat deze instellingen doorgaans op clusterniveau worden beheerd. Als u meerdere machines hebt die niet zijn geclusterd, of als u deze instellingen op machineniveau beheert, moet stap # 1 op elke ESA worden uitgevoerd.

1. Navigeer vanuit de ESA UI naar Security Services > Cisco IronPort Email Encryption.
2. Schakel het selectievakje in om Cisco IronPort-e-mailcodering in te schakelen.
3. Accepteer de licentieovereenkomst voor eindgebruikers (EULA) en de licentieovereenkomst voor e-mailcodering van Cisco IronPort.
4. Klik in de Algemene instellingen voor e-mailcodering op Instellingen bewerken...
 - Geef het e-mailadres op voor de beheerder/persoon die de primaire RES-beheerder voor het account is. Dit e-mailaccount wordt gekoppeld aan het beheer van de RES-omgeving voor het bedrijf.
 - Optioneel: De standaard maximale berichtgrootte om te versleutelen is 10M. U kunt de grootte op dit moment vergroten of verkleinen als u dat wilt.
 - Optioneel: Als u een proxy hebt die de ESA moet doorlopen om via HTTPS verbinding te maken met RES, voegt u de nodige proxy- en authenticatie-instellingen toe om deze door de proxy te laten gaan.
5. Verzend en verbind uw configuratiewijzigingen.

Op dit punt moet u de "Algemene instellingen voor e-mailcodering" op iets als dit instellen, maar nog geen profielen vermeld:

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. Registreer uw ESA(s) en uw organisatie bij RES

Stap #2 maakt voornamelijk deel uit van de ESA-beheerconsole.

 Opmerking: ESA-registratiegegevens zijn ook te vinden in de volgende TechNote: [Cisco RES: Account Provisioning for Virtual, Hosted, and Hardware ESA Configuration Voorbeeld](#)

Stuur een e-mail rechtstreeks naar RES: stg-cres-provisioning@cisco.com.

Om een CRES-account aan te maken voor het (de) coderingsprofiel(en) van uw ESA, dient u ons de volgende informatie te verstrekken:

1. Naam van account (Geef de exacte bedrijfsnaam op, omdat u wilt dat deze wordt vermeld.)
 1. Voor Cloud Email Security (CES)/Hosted klantaccounts, gelieve uw accountnaam te vermelden om te eindigen als "<Accountnaam> HOSTED"
2. E-mailadres(sen) voor de accountbeheerder (geef het bijbehorende e-mailadres van de beheerder op)
3. Voltooi serienummer(s) van het apparaat
 1. Een serienummer van het toestel kan worden gevonden vanuit de ESA GUI (Systeembeheer > Functiesleutels) of ESA CLI via de opdracht 'versie'. Het verstrekken van een licentie voor een virtueel licentienummer (VLN) of een productactiveringssleutel (PAK) is niet aanvaardbaar, omdat een volledig serienummer van het apparaat vereist is voor het beheer van de CRES-account.
4. Domeinnamen die voor beheerdoeleinden aan de CRES-account moeten worden toegewezen

Opmerking: als u al een CRES-account hebt, geeft u de bedrijfsnaam of het bestaande CRES-accountnummer op. Dit zorgt ervoor dat alle nieuwe serienummers van het apparaat aan het juiste account worden toegevoegd en voorkomt duplicatie van bedrijfsinformatie en provisioning.

Wees ervan verzekerd dat als u e-mailt over het leveren van een CRES-account, we binnen één (1) werkdag reageren. Als u onmiddellijk ondersteuning en hulp nodig hebt, opent u een ondersteuningsverzoek met Cisco TAC. Dit kan via Support Case Manager (<https://mycase.cloudapps.cisco.com/case>) of telefonisch (<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>).

 Opmerking: nadat u dit verzoek hebt gemaild, kan het een dag duren voordat uw RES-account van het bedrijf is gemaakt (als deze nog niet is gemaakt) en de S / N's worden toegevoegd. De taak "Voorziening", in Stap #3, zal niet werken totdat dit is voltooid.

3. Coderingsprofielen op de ESA(s) aanmaken

 Opmerking: als u meerdere ESA's in een cluster hebt, hoeft stap #1 slechts eenmaal te worden uitgevoerd, omdat deze instellingen doorgaans op clusterniveau worden beheerd.



Als u meerdere machines hebt die niet zijn geclusterd, of als u deze instellingen op machineniveau beheert, moet stap # 1 op elke ESA worden uitgevoerd.

Een coderingsprofiel geeft aan hoe versleutelde berichten moeten worden verzonden. Een organisatie moet bijvoorbeeld mogelijk enveloppen met hoge beveiliging verzenden voor een segment van de ontvangers, zoals degenen waarvan ze weten dat ze vaak zeer gevoelige gegevens naar verzenden. Dezelfde organisatie kan andere segmenten van hun ontvangende gemeenschap hebben die minder gevoelige informatie ontvangen, en die misschien ook minder geduldig zijn met het moeten verstrekken van gebruikersnaam en wachtwoord om gecodeerde e-mail te ontvangen. Die ontvangers zouden goede kandidaten zijn voor een laag beveiligde envelop. Met meerdere coderingsprofielen kan de organisatie het gecodeerde berichtformaat aanpassen aan het publiek. Aan de andere kant kunnen veel organisaties prima zijn met slechts één coderingsprofiel.

Voor dit document geven we een voorbeeld van het maken van drie coderingsprofielen met de naam "CRES_HIGH", "CRES_MED" en "CRES_LOW".

1. Navigeer vanuit de ESA UI naar Security Services > Cisco IronPort Email Encryption.
2. Klik op "Encryptieprofiel toevoegen..."
3. Het menu Coderingsprofiel wordt geopend en u kunt uw eerste coderingsprofiel "CRES_HIGH" noemen.
4. Selecteer "High Security" voor het envelop Message Security (Beveiliging van envelop) als dit nog niet is geselecteerd.
5. Klik op Verzenden om dit profiel op te slaan.

Encryption Profile Settings	
Profile Name:	CRES_HIGH
Key Server Settings	
Key Service Type:	Cisco Registered Envelope Service
Proxy:	A proxy server is not currently configured.
Cisco Registered Envelope Service URL:	https://res.cisco.com
	Advanced Advanced key server settings
Envelope Settings	
	Example Envelope
Envelope Message Security:	☒ High Security <i>Recipient must enter a passphrase to open the encrypted message, even if credentials are cached ("Remember Me" selected).</i> ☐ Medium Security <i>No passphrase entry required if recipient credentials are cached ("Remember Me" selected).</i> ☐ No Passphrase Required <i>The recipient does not need a passphrase to open the encrypted message.</i>
Logo Link:	☒ No link ☐ Custom link URL: <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:	☒ Enable Read Receipts
	Advanced Advanced envelope settings
Message Settings	
	Example Message
End-User Controls:	☐ Enable Secure Reply All ☐ Enable Secure Message Forwarding
Notification Settings	
Localized Envelopes:	☐ 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: [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:	securedoc_\${date}T\${time}.html

Herhaal vervolgens stap 2-5 om "CRES_MED" en "CRES_LOW" te maken - wijzig gewoon de keuzerondje voor de envelopberichtenbeveiliging voor elk profiel.

- Kies voor het CRES_HIGH-profiel de knop "High Security".
- Kies voor het CRES_MED-profiel de knop "Medium Security".
- Kies voor het CRES_LOW-profiel de knop "Geen wachtwoord vereist"

U zult merken dat er opties zijn om Leesbonnen in te schakelen, Veilig Alles beantwoorden in te schakelen en Veilig doorsturen van berichten in te schakelen. Als u in Envelopinstellingen op de koppeling "Geavanceerd" klikt, kunt u een van de drie symmetrische coderingsalgoritmen selecteren en specificeren dat de envelop wordt verzonden zonder de Java-coderingsapplet.

Rechts van Envelopinstellingen ziet u de hyperlink "Voorbeeld bericht". Als hierop wordt geklikt, toont dit een voorbeeld van de Secure Message Envelope - wat de ontvanger in zijn e-mail zal zien nadat hij de HTML-bijlage heeft geopend.

Leesbonnen betekent dat de afzender van het gecodeerde bericht een e-mail van CRES ontvangt wanneer de ontvanger het beveiligde bericht opent (wat betekent dat de ontvanger de symmetrische sleutel heeft neergehaald en het bericht heeft ontsleuteld).

Rechts van de Berichtinstellingen ziet u de hyperlink "Voorbeeld Bericht". Als hierop wordt geklikt, toont dit u hoe het geopende bericht eruit zal zien - wat de ontvanger zal zien zodra hij de nodige informatie in de envelop heeft verstrekt en het versleutelde bericht heeft geopend.

Klik altijd op Verzenden en breng wijzigingen aan.

De rij in de tabel toont dan een knop "Voorziening". De knop Voorziening verschijnt pas nadat u wijzigingen hebt vastgelegd.

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		

Klik nogmaals op de knop Voorziening, dit werkt alleen nadat uw RES-account van het bedrijf is gemaakt en de S/N van het apparaat aan uw account is toegevoegd. Als de RES-rekening aan het ESA is gekoppeld, zal het voorzieningsproces relatief snel verlopen. Als dat niet het geval is, moet dat proces eerst worden afgerond.

Zodra de provisioning is voltooid, wordt op de pagina E-mailcodering van Cisco IronPort het profiel weergegeven zoals voorzien.

4. Preventie van gegevensverlies (DLP) inschakelen

1. Navigeer vanuit de ESA-gebruikersinterface naar Security Services > Data Loss Prevention.
2. Klik op Inschakelen... om DLP in te schakelen.
3. Accepteer de EULA, Data Loss Prevention License Agreement.
4. Klik op het selectievakje voor het inschakelen van overeenkomende logboekregistratie.

- Schakel het selectievakje voor automatische updates inschakelen in.
- Klik op Verzenden.

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

Updates voor de DLP-engine en vooraf gedefinieerde classificaties voor het matchen van inhoud op uw toestel zijn onafhankelijk van updates voor andere beveiligingsservices. De 3-5 minuten reguliere Talos handtekening updates zijn verschillend en omvatten niet het bijwerken van DLP beleid en woordenboeken. Updates moeten hier worden ingeschakeld.

Wanneer "Logboekregistratie voor overeenkomende inhoud" is ingeschakeld, kan Berichtentracking de inhoud weergeven van de e-mail die de overtreding heeft veroorzaakt. Hier is een voorbeeld van Message Tracking met de e-mailinhoud die de DLP-overtreding heeft veroorzaakt. Op deze manier kan een beheerder precies weten welke gegevens een specifiek DLP-beleid hebben geactiveerd.

Message Details	
Summary	DLP Matched Content
MESSAGE ID "153" MATCHED DLP POLICY: custom_policy	
Violation Severity:	MEDIUM (Risk Factor: 50)
attachment.xls:	Credit Cards - 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 540410R95R654RR1 110 R/2009

Overtreding van

gegevensverliespreventie

5. Berichtacties voor het voorkomen van gegevensverlies maken

DLP-quarantaines maken

Als u een kopie wilt bewaren van berichten die het DLP-beleid schenden, kunt u individuele beleidsquarantaines maken voor elk type beleidsovertreding. Dit is vooral handig bij het uitvoeren van een 'transparante' POV, waarbij uitgaande berichten die het DLP-beleid schenden worden gelogd en afgeleverd, maar er geen actie wordt ondernomen met betrekking tot de berichten.

- Navigeer op de SMA naar E-mail > Berichtenquarantaine > Beleid, virus en uitbraakquarantaine

- Dit is hoe de quarantainetabel eruit moet zien voordat we beginnen:

Policy, Virus and Outbreak Quarantines					
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size
Spam Analysis	Advanced Malware Protection	0	Release 1 hour after Release	N/A	0
Outbreak (Triggered by Rule Summary)	Outbreak	0	Release 1 hour after Release	23 Jan 2020 14:43 (GMT +05:00)	0
Outbreak	Outbreak	0	Release 1 hour after Release	N/A	0
Outbreak (Triggered by Rule Summary)	Outbreak	0	Release 1 hour after Release	N/A	0
Outbreak	Outbreak	0	Release 1 hour after Release	N/A	0

Beleidsvirus en uitbraak quarantaine

3. Klik op de knop "Beleidsquarantaine toevoegen" en maak een quarantaine die door het DLP-beleid moet worden gebruikt.

Hieronder vindt u een voorbeeld van een quarantaine gemaakt voor een medium DLP overtreding. Segmentatie van quarantaines is mogelijk en kan gewenst zijn voor meerdere DLP-regels:

Add Quarantine

Settings	
Quarantine Name:	DLP Quarantine Violations
Retention Period:	14 Days
Default Action:	☒ Delete ☐ Release
	☒ 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

Voorbeeld DLP-quarantaine

Informatie over DLP-berichtacties

DLP-berichtacties beschrijven welke acties de ESA zal ondernemen wanneer het een DLP-overtreding in een uitgaande e-mail detecteert. U kunt primaire en secundaire DLP-acties opgeven en verschillende acties kunnen worden toegewezen voor verschillende overtredingstypen en -ernst.

Primaire acties zijn onder meer:

- leveren
- Afwijzing
- quarantaine

Voor een alleen-lezen-status waarbij DLP-overtredingen worden geregistreerd en gerapporteerd, maar de berichten niet worden gestopt / in quarantaine geplaatst of gecodeerd, wordt de actie Bezorgen het vaakst gebruikt.

Secundaire acties zijn onder meer:

- Het verzenden van een kopie naar een aangepaste quarantaine of de 'Policy'-quarantaine.
- Codeer het bericht. Het apparaat versleutelt alleen de berichttekst. Het versleutelt de berichtkoppen niet.
- De koptekst van het onderwerp wijzigen.
- Het toevoegen van disclaimer tekst / HTML aan het bericht.
- Het bericht verzenden naar een alternatieve bestemmingsmailhost.

- BCC-kopieën van het bericht verzenden.
- DLP-overtredingsmelding verzenden naar de afzender en/of andere contactpersonen.

Deze acties sluiten elkaar niet uit - u kunt sommige ervan combineren binnen verschillende DLP-beleidsregels voor verschillende verwerkingsbehoeften voor verschillende gebruikersgroepen.

We gaan de volgende DLP-acties implementeren: Encrypt

Deze acties gaan ervan uit dat encryptie is gelicentieerd en geconfigureerd op de ESA en drie profielen zijn gemaakt voor hoge, gemiddelde en lage beveiliging, zoals in de eerdere secties is gedaan:

- CRES_HOOG
- CRES_MED
- CRES_LAAG

De DLP-berichtacties maken

1. Ga naar Mail Policies > DLP Message Customisations.
2. Klik op de knop "Berichtactie toevoegen" en voeg de volgende DLP-acties toe. Zorg ervoor dat u de wijziging vastlegt na het verzenden van het bericht

Add Message Action

Name:

Description:

Message Action:

☒ Enable Encryption

Encryption Rule:

(See TLS settings at Mail Policies > Destination Controls)

Encryption Profile:

Encrypted Message Subject:

☒ Send a copy of message to quarantine.

[Advanced](#) This section contains settings for Message modifications, message delivery and DLP notifications.

Berichtenactie

6. Beleidsregels voor het voorkomen van gegevensverlies opstellen

Een DLP-beleid omvat:

- Een reeks voorwaarden die bepalen of een uitgaand bericht gevoelige gegevens bevat
- De acties die moeten worden ondernomen wanneer een bericht dergelijke gegevens bevat.

1. Navigeer naar: Mail Policies > DLP Policy Manager
2. Klik op 'DLP-beleid toevoegen'
3. Open de "Regulatory Compliance"-openbaarmakingsdriehoek.

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](#)

DLP-beleidssjabloon

4. Klik voor het PCI-beleid op de knop "Toevoegen" links van 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:	This policy identifies cardholder data, including but not limited to Primary Account Number (PAN), expiration dates, and magnetic stripe data.
Filter Senders and Recipients:	Restrict this DLP policy by specific recipients and senders.
Filter Attachments:	Restrict this DLP policy to detect specific attachment types.
Filter Message Tags:	Restrict this DLP policy to detect message tags.

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](#)

PCI-DSS voorbeeld DLP regel

5. Selecteer voor het incident met kritieke ernst de actie "Medium versleutelen en leveren" die we eerder hebben geconfigureerd. We kunnen de lagere ernst van de incidenten veranderen, maar laten we ze nu onze kritieke ernst van het incident laten erven. Indienen en vervolgens de wijziging doorvoeren.

7. DLP-beleid toepassen op een uitgaand e-mailbeleid

1. Navigeer naar: E-mailbeleid > Beleid voor uitgaande e-mail

2. Klik op de controlecel voor DLP voor het standaardbeleid. Het leest "Uitgeschakeld" als u het nog niet hebt ingeschakeld.
3. Wijzig de pulldown-knop van DLP uitschakelen in DLP inschakelen en u krijgt onmiddellijk het DLP-beleid te zien dat u zojuist hebt gemaakt.
4. Klik op het selectievakje "Alles inschakelen". Verzenden en dan de wijzigingen vastleggen.

Conclusie

Samenvattend hebben we de nodige stappen getoond om een Cisco Email Security Appliance voor te bereiden op het verzenden van een gecodeerde e-mail:

1. E-mailcodering van Cisco IronPort inschakelen
2. Registreer uw ESA(s) en uw organisatie bij RES
3. Coderingsprofielen maken
4. DLP inschakelen
5. DLP-berichtacties maken
6. DLP-beleid maken
7. DLP-beleid toepassen op een uitgaand e-mailbeleid

Meer informatie is beschikbaar in de ESA-gebruikershandleiding die overeenkomt met uw ESA-software release. De gebruikershandleidingen zijn beschikbaar via de volgende link:

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

Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.