

Best Practices-Leitfaden für Data Loss Prevention und Verschlüsselung

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Best Practice-Leitfaden für Data Loss Prevention und Verschlüsselung - Best Practices](#)

[1. Aktivieren Sie Cisco IronPort Email Encryption auf den ESA\(s\)](#)

[2. Registrieren Sie Ihre ESA\(s\) und Ihre Organisation bei RES](#)

[3. Erstellen von Verschlüsselungsprofilen auf den ESA\(s\)](#)

[4. Schutz vor Datenverlust \(Data Loss Prevention, DLP\) aktivieren](#)

[5. Erstellen von Nachrichtenaktionen zum Schutz vor Datenverlust](#)

[6. Erstellen von Richtlinien zum Schutz vor Datenverlust](#)

[7. Anwenden von SvD-Policys auf Richtlinien für ausgehende E-Mails](#)

[Schlussfolgerung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden Best Practices für den Schutz vor Datenverlust (DLP) und die Verschlüsselung für Cisco Email Security beschrieben.

In diesem Dokument wird die Einrichtung der Nachrichtenverschlüsselung mithilfe der Cisco E-Mail Security Appliance (ESA) und des Cloud-basierten Cisco Registered Envelope Service (RES) erläutert. Mithilfe der Nachrichtenverschlüsselung können Kunden einzelne Nachrichten sicher über das öffentliche Internet versenden. Hierzu stehen verschiedene Arten von Richtlinien zur Verfügung, darunter Content-Filterung und DLP. Die Erstellung dieser Richtlinien wird in anderen Dokumenten dieser Reihe behandelt. Dieses Dokument konzentriert sich darauf, die ESA darauf vorzubereiten, verschlüsselte E-Mails zu senden, damit Richtlinien die Verschlüsselung als Aktion verwenden können.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

In diesem Dokument werden die folgenden Schritte erläutert:

1. Aktivieren von Cisco IronPort Email Encryption
2. Registrieren Sie Ihre ESA(s) und Ihre Organisation mit RES
3. Erstellen von Verschlüsselungsprofilen
4. Aktivieren von DLP
5. DLP-Nachrichtenaktionen werden erstellt
6. Erstellen von SvD-Policys
7. Anwenden von SvD-Policys auf eine ausgehende E-Mail-Policy

Sobald diese Schritte erfolgreich abgeschlossen wurden, kann der ESA-Administrator erfolgreich eine Richtlinie erstellen, die die Verschlüsselung als Aktion verwendet.

Cisco IronPort Email Encryption wird auch als RES-Verschlüsselung bezeichnet. RES ist der Name, den wir für die "Schlüsselserver" in der Cisco Cloud verwenden. Die RES-Verschlüsselungslösung verwendet eine Verschlüsselung mit symmetrischem Schlüssel. Das bedeutet, dass der Schlüssel, der zur Verschlüsselung der Nachricht verwendet wird, derselbe Schlüssel ist, der auch zur Entschlüsselung der Nachricht verwendet wird. Jede verschlüsselte Nachricht verwendet einen eindeutigen Schlüssel, der es dem Absender ermöglicht, nach dem Senden eine präzise Kontrolle über eine Nachricht zu haben - um sie beispielsweise zu sperren oder zu verfallen, sodass der Empfänger sie nicht mehr öffnen kann -, ohne andere Nachrichten zu beeinträchtigen. Bei der Verschlüsselung einer Nachricht speichert die ESA den Verschlüsselungsschlüssel und Metadaten zu jeder verschlüsselten Nachricht in CRES.

Die ESA kann eine Nachricht auf vielfältige Weise verschlüsseln, z. B. über ein "Flag" (z. B. den Inhalt eines Betreffs), über einen Content-Filter-Abgleich oder über eine SvD-Policy. Wenn die ESA beschließt, eine Nachricht zu verschlüsseln, tut sie dies mit einem angegebenen "Verschlüsselungsprofil", das unter "Sicherheitsdienste > Cisco IronPort E-Mail-Verschlüsselung" erstellt wurde - der Tabelle mit dem Namen "E-Mail-Verschlüsselungsprofile". Standardmäßig sind keine Verschlüsselungsprofile vorhanden. Dies wird in Abschnitt 3. Erstellen von Verschlüsselungsprofilen erläutert.

Best Practice-Leitfaden für Data Loss Prevention und Verschlüsselung - Best Practices

1. Aktivieren Sie Cisco IronPort Email Encryption auf den ESA(s)

 Anmerkung: Wenn Sie mehrere ESAs in einem Cluster haben, muss Schritt #1 nur einmal ausgeführt werden, da diese Einstellungen in der Regel auf Cluster-Ebene verwaltet werden. Wenn Sie mehrere Computer haben, die nicht geclustert sind, oder wenn Sie diese Einstellungen auf Computerebene verwalten, sollte Schritt #1 auf jeder ESA ausgeführt werden.

1. Navigieren Sie in der ESA-Benutzeroberfläche zu Security Services > Cisco IronPort Email Encryption.
2. Aktivieren Sie das Kontrollkästchen, um Cisco IronPort Email Encryption zu aktivieren.
3. Akzeptieren Sie den Endbenutzer-Lizenzvertrag (EULA) und den Cisco IronPort Email Encryption-Lizenzvertrag.
4. Klicken Sie in den globalen Einstellungen für die E-Mail-Verschlüsselung auf Einstellungen bearbeiten...
 - Geben Sie die E-Mail-Adresse für den Administrator/die Person an, die der primäre RES-Administrator für das Konto ist. Dieses E-Mail-Konto wird mit der Administration der RES-Umgebung für das Unternehmen verknüpft.
 - Optional: Die standardmäßige maximale Nachrichtengröße für die Verschlüsselung beträgt 10 MB. Sie können die Größe zu diesem Zeitpunkt erhöhen oder verringern, wenn Sie möchten.
 - Optional: Wenn Sie über einen Proxy verfügen, den die ESA durchlaufen muss, um über HTTPS eine Verbindung zu RES herzustellen, fügen Sie den erforderlichen Proxy und die Authentifizierungseinstellungen hinzu, damit die ESA über den Proxy kommunizieren kann.
5. Senden und bestätigen Sie Ihre Konfigurationsänderungen.

An dieser Stelle sollten Sie die Einstellung "Email Encryption Global Settings" (Globale Einstellungen für E-Mail-Verschlüsselung) wie folgt sehen, allerdings ohne dass bisher Profile aufgelistet wurden:

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. Registrieren Sie Ihre ESA(s) und Ihre Organisation bei RES

Der Schritt #2 wird in erster Linie außerhalb der ESA-Administrationskonsole ausgeführt.



Anmerkung: Informationen zur ESA-Registrierung finden Sie auch in den folgenden TechNote: [Cisco RES: Kontobereitstellung für Virtual, Hosted und Hardware - ESA-Konfigurationsbeispiel](#)

Senden Sie eine E-Mail direkt an RES: stg-cres-provisioning@cisco.com.

Um ein CRES-Konto für die Verschlüsselungsprofile Ihrer ESA einzurichten, geben Sie die folgenden Informationen an:

1. Kontoname (Bitte geben Sie den genauen Firmennamen an, da dieser aufgeführt werden muss.)
 1. Bei Cloud Email Security(CES)-/gehosteten Kundenkonten geben Sie bitte den Namen Ihres Kontos an, um als "<Account Name> HOSTED" zu enden.
2. E-Mail-Adresse(n) für den Account Admin (Bitte geben Sie die entsprechende Admin-E-Mail-Adresse an)
3. Vollständige Seriennummer(n) der Appliance
 1. Die Seriennummer einer Einheit kann über die ESA-GUI (Systemverwaltung > Feature-Schlüssel) oder über die ESA-CLI über den Befehl "version" ermittelt werden. Die Angabe einer VLN- (Virtual License Number) oder PAK-Lizenz (Product Activation Key) ist nicht akzeptabel, da für die CRES-Kontoverwaltung eine vollständige Seriennummer der Appliance erforderlich ist.
4. Domännennamen, die dem CRES-Konto zu Verwaltungszwecken zugeordnet werden sollen

Anmerkung: Wenn Sie bereits über ein CRES-Konto verfügen, geben Sie bitte den Firmennamen oder die bestehende CRES-Kontonummer an. Auf diese Weise wird sichergestellt, dass neue Seriennummern der Appliances dem richtigen Konto hinzugefügt werden, und eine Duplizierung von Unternehmensinformationen und Provisioning wird vermieden.

Wenn Sie eine E-Mail bezüglich der Bereitstellung eines CRES-Kontos senden, erhalten Sie innerhalb eines (1) Werktags von uns eine Antwort. Wenn Sie sofortigen Support und Unterstützung benötigen, eröffnen Sie bitte eine Support-Anfrage beim Cisco TAC. Dies kann über den Support Case Manager (<https://mycase.cloudapps.cisco.com/case>) oder telefonisch (<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>) erfolgen.

 Anmerkung: Nachdem Sie diese Anfrage per E-Mail gesendet haben, kann es einen Tag dauern, bis Ihr Firmen-RES-Konto erstellt (sofern es nicht bereits erstellt wurde) und die S/Ns hinzugefügt wurden. Die Aufgabe "Bereitstellen" in Schritt #3 funktioniert erst, wenn diese abgeschlossen ist.

3. Erstellen von Verschlüsselungsprofilen auf den ESA(s)

 Anmerkung: Wenn Sie mehrere ESAs in einem Cluster haben, muss Schritt #1 nur einmal ausgeführt werden, da diese Einstellungen in der Regel auf Cluster-Ebene verwaltet werden. Wenn Sie mehrere Computer haben, die nicht geclustert sind, oder wenn Sie diese Einstellungen auf Computerebene verwalten, sollte Schritt #1 auf jeder ESA ausgeführt werden.

Ein Verschlüsselungsprofil legt fest, wie verschlüsselte Nachrichten gesendet werden sollen. So kann es z. B. vorkommen, dass ein Unternehmen Hochsicherheits-Umschläge für ein Segment seiner Empfänger versenden muss, z. B. solche, von denen bekannt ist, dass sie häufig sehr vertrauliche Daten an diese senden. Dieselbe Organisation hat möglicherweise andere Segmente ihrer Empfänger-Community, die weniger vertrauliche Informationen erhalten und die möglicherweise auch weniger geduldig sind, wenn sie Benutzer-ID und Passwort angeben müssen, um verschlüsselte E-Mails zu empfangen. Diese Empfänger wären gute Kandidaten für einen Umschlag vom Typ "Niedrige Sicherheit". Mehrere Verschlüsselungsprofile ermöglichen es dem Unternehmen, das Format der verschlüsselten Nachricht an die Zielgruppe anzupassen. Auf der anderen Seite können viele Unternehmen mit nur einem Verschlüsselungsprofil zufrieden sein.

In diesem Dokument wird ein Beispiel für die Erstellung von drei Verschlüsselungsprofilen mit den Namen "CRES_HIGH", "CRES_MED" und "CRES_LOW" gezeigt.

1. Navigieren Sie in der ESA-Benutzeroberfläche zu Security Services > Cisco IronPort Email Encryption.
2. Klicken Sie auf "Verschlüsselungsprofil hinzufügen..."
3. Das Menü für das Verschlüsselungsprofil wird geöffnet, und Sie können Ihrem ersten Verschlüsselungsprofil den Namen "CRES_HIGH" geben.
4. Wählen Sie für die Nachrichtensicherheit des Umschlags die Option "Hohe Sicherheit" aus,

wenn diese Option noch nicht ausgewählt ist.

5. Klicken Sie auf Senden, um dieses Profil zu speichern.

Encryption Profile Settings	
Profile Name:	CRES_HIGH
Key Server Settings	
Key Service Type:	Cisco Registered Envelope Service
Proxy:	<i>A proxy server is not currently configured.</i>
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

Wiederholen Sie anschließend die Schritte 2-5, um "CRES_MED" und "CRES_LOW" zu erstellen. Ändern Sie einfach das Optionsfeld für die Umschlagsnachrichtensicherheit für jedes Profil.

- Wählen Sie für das CRES_HIGH-Profil das Optionsfeld "Hohe Sicherheit".
- Wählen Sie für das CRES_MED-Profil das Optionsfeld "Mittlere Sicherheit".
- Wählen Sie für das Profil CRES_LOW das Optionsfeld "Kein Kennwort erforderlich".

Sie sehen, dass es Optionen zum Aktivieren von Lesebestätigungen, zum Aktivieren der Funktion "Sichere Antwort an alle" und zum Aktivieren der sicheren Nachrichtenweiterleitung gibt. Wenn Sie in den Umschlageinstellungen auf den Link "Erweitert" klicken, können Sie einen von drei symmetrischen Verschlüsselungsalgorithmen auswählen und angeben, dass der Umschlag ohne das Java-Verschlüsselungs-Applet gesendet wird.

Rechts neben den Umschlageinstellungen wird der Hyperlink "Beispielnachricht" angezeigt. Wenn Sie darauf klicken, wird Ihnen ein Beispiel des Umschlags für sichere Nachrichten angezeigt - was der Empfänger in seiner E-Mail sehen wird, nachdem er den HTML-Anhang geöffnet hat.

Lesebestätigungen bedeutet, dass der Absender der verschlüsselten Nachricht eine E-Mail von CRES erhält, wenn der Empfänger die sichere Nachricht öffnet (d. h. der Empfänger hat den symmetrischen Schlüssel heruntergezogen und die Nachricht entschlüsselt).

Rechts neben den Nachrichteneinstellungen sehen Sie den Hypertext-Link "Example Message" (Beispielnachricht). Wenn Sie darauf klicken, wird Ihnen angezeigt, wie die geöffnete Nachricht aussehen wird - was der Empfänger sehen wird, wenn er die erforderlichen Informationen in den Umschlag eingegeben und die verschlüsselte Nachricht geöffnet hat.

Denken Sie immer daran, auf Senden zu klicken und Änderungen zu bestätigen.

Die Zeile in der Tabelle zeigt dann die Schaltfläche "Provisioning" (Bereitstellung). Die Schaltfläche "Provisioning" wird erst angezeigt, nachdem Sie die Änderungen bestätigt haben.

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		

Klicken Sie erneut auf die Schaltfläche "Provisioning" (Bereitstellung). Dies funktioniert erst, nachdem Ihr Firmen-RES-Konto erstellt wurde und die Appliance-Systemnummern zu Ihrem Konto hinzugefügt wurden. Wenn das RES-Konto mit der ESA verbunden ist, erfolgt der Bereitstellungsprozess relativ schnell. Ist dies nicht der Fall, muss dieser Prozess zuerst abgeschlossen werden.

Nach Abschluss der Bereitstellung wird auf der Seite für die Cisco IronPort E-Mail-Verschlüsselung das bereitgestellte Profil angezeigt.

4. Schutz vor Datenverlust (Data Loss Prevention, DLP) aktivieren

1. Navigieren Sie in der ESA-Benutzeroberfläche zu Security Services > Data Loss Prevention.
2. Klicken Sie auf Aktivieren..., um SvD zu aktivieren.
3. Akzeptieren Sie die EULA, Data Loss Prevention-Lizenzvereinbarung.
4. Klicken Sie auf das Kontrollkästchen für "Protokollierung zugeordneter Inhalte aktivieren".
5. Aktivieren Sie das Kontrollkästchen Automatische Updates aktivieren.
6. Klicken Sie auf Senden.

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 für die SvD-Engine und vordefinierte Klassifizierungen für die Inhaltszuordnung auf Ihrer Appliance sind unabhängig von Updates für andere Sicherheitsdienste. Die regelmäßigen 3-5-minütigen Signatur-Updates von Talos unterscheiden sich und beinhalten keine Aktualisierung der DLP-Richtlinien und -Wörterbücher. Updates müssen hier aktiviert sein.

Wenn die Protokollierung zugeordneter Inhalte aktiviert ist, kann mit der Nachrichtenverfolgung der Inhalt der E-Mail angezeigt werden, die die Verletzung verursacht hat. Das nachfolgende Beispiel zeigt den E-Mail-Inhalt, der die SvD-Verletzung verursacht hat. Auf diese Weise kann ein Administrator genau wissen, welche Daten eine bestimmte DLP-Richtlinie ausgelöst haben.

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 540410R9KRAK4ARR1 110 R/2009

Schutzes vor Datenverlust

Verletzung des

5. Erstellen von Nachrichtenaktionen zum Schutz vor Datenverlust

SvD-Quarantänen erstellen

Wenn Sie eine Kopie der Nachrichten behalten möchten, die gegen SvD-Richtlinien verstoßen, können Sie für jede Art von Richtlinienverletzung eine individuelle Policy-Quarantäne erstellen. Dies ist besonders nützlich, wenn ein "transparenter" POV ausgeführt wird, bei dem ausgehende Nachrichten, die gegen DLP-Richtlinien verstoßen, protokolliert und übermittelt werden, aber keine

Maßnahmen hinsichtlich der Nachrichten ergriffen werden.

1. Navigieren Sie auf der SMA zu E-Mail > Nachrichtenquarantäne > Richtlinie, Virus und Outbreak-Quarantäne

Policy, Virus and Outbreak 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	Outbreak	0	Retain 1 hour then Release	23 Jul 2020 14:43 (GMT+00:00)	0	
[Change by Rule Summary]						
Policy	Policy	0	Retain 15 days then Delete	N/A	0	
Unquarantined	Unquarantined	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, Antismash & Outbreak quarantines is 20G.

2. So sollte die Quarantäne-Tabelle aussehen, bevor wir beginnen:
Richtlinien-Virus und Outbreak-Quarantäne
3. Klicken Sie auf die Schaltfläche "Add Policy Quarantine" (Richtlinienquarantäne hinzufügen), und erstellen Sie eine Quarantäne, die von den SvD-Richtlinien verwendet werden soll.

Im Folgenden finden Sie ein Beispiel für eine Quarantäne bei einer Verletzung des DLP-Typs "Medium". Eine Segmentierung der Quarantänen ist möglich und kann für mehrere SvD-Regeln gewünscht werden:

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

Cancel

Submit

Beispiel für SvD-Quarantäne

Info zu SvD-Nachrichtenaktionen

SvD-Nachrichtenaktionen beschreiben, welche Aktionen die ESA ausführt, wenn eine SvD-Verletzung in einer ausgehenden E-Mail erkannt wird. Sie können primäre und sekundäre SvD-Aktionen angeben, und es können verschiedene Aktionen für unterschiedliche Verletzungstypen und -schweregrade zugewiesen werden.

Zu den wichtigsten Maßnahmen gehören:

- Zustellen
- Verwerfen
- Quarantäne

In einem schreibgeschützten Zustand, in dem SvD-Verletzungen protokolliert und gemeldet werden, die Nachrichten aber nicht gestoppt/in Quarantäne gestellt oder verschlüsselt werden, wird meistens die Deliver-Aktion verwendet.

Zu den sekundären Aktionen gehören:

- Eine Kopie wird an eine benutzerdefinierte Quarantäne oder die Quarantäne der Richtlinie gesendet.
- Verschlüsseln der Nachricht Die Appliance verschlüsselt nur den Nachrichtentext. Die Nachrichtenheader werden nicht verschlüsselt.
- Ändern des Subject-Headers.
- Text/HTML für Haftungsausschluss zur Nachricht hinzufügen.
- Die Nachricht wird an einen alternativen Ziel-Mailhost gesendet.
- BCC-Kopien der Nachricht werden gesendet.
- SvD-Verletzungsbenachrichtigung wird an den Absender und/oder andere Kontakte gesendet.

Diese Aktionen schließen sich nicht gegenseitig aus. Sie können einige davon innerhalb verschiedener SvD-Richtlinien kombinieren, um verschiedene Verarbeitungsanforderungen für verschiedene Benutzergruppen zu erfüllen.

Wir implementieren die folgenden DLP-Aktionen: Verschlüsseln

Bei diesen Aktionen wird davon ausgegangen, dass die Verschlüsselung auf der ESA lizenziert und konfiguriert ist und drei Profile für die hohe, mittlere und niedrige Sicherheit erstellt wurden, wie in den vorherigen Abschnitten beschrieben:

- CRES_HOCH
- CRES_MED
- CRES_LOW

Aktionen für SvD-Meldungen erstellen

1. Gehen Sie zu Mail-Policys > SvD-Nachrichtenanpassungen.
2. Klicken Sie auf die Schaltfläche "Nachrichtenaktion hinzufügen", und fügen Sie die folgenden SvD-Aktionen hinzu. Bestätigen Sie die Änderung, nachdem Sie die Nachrichtenaktion gesendet haben.

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

6. Erstellen von Richtlinien zum Schutz vor Datenverlust

Eine SvD-Richtlinie umfasst:

- Ein Satz von Bedingungen, die bestimmen, ob eine ausgehende Nachricht vertrauliche Daten enthält.
- Die Aktionen, die ausgeführt werden müssen, wenn eine Nachricht solche Daten enthält.

1. Navigieren Sie zu: Mail-Policys > SvD-Policy-Manager
2. Klicken Sie auf "SvD-Policy hinzufügen".
3. Öffnen Sie das Dreieck "Erfüllung gesetzlicher Auflagen".

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

SvD-Richtlinienvorlage

4. Klicken Sie für PCI-Richtlinien auf die Schaltfläche "Hinzufügen" links neben 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 Beispiel-DLP-Regel

5. Wählen Sie für den Vorfall mit kritischem Schweregrad die Aktion "Medium verschlüsseln und zustellen", die Sie zuvor konfiguriert haben. Wir könnten die Zwischenfälle mit niedrigerem Schweregrad ändern, aber im Moment sollten sie unseren Zwischenfall mit kritischem Schweregrad erben. Senden und bestätigen Sie die Änderung.

7. Anwenden von SvD-Policys auf Richtlinien für ausgehende E-Mails

1. Navigieren Sie zu: Mail-Policys > Richtlinien für ausgehende Mails
2. Klicken Sie auf die Kontrollzelle für SvD für die Standardrichtlinie. Es wird "Disabled" (Deaktiviert) angezeigt, wenn Sie es noch nicht aktiviert haben.
3. Ändern Sie die Pulldown-Schaltfläche Disable DLP (SvD deaktivieren) in Enable DLP (SvD aktivieren). Daraufhin wird sofort die SvD-Policy angezeigt, die Sie gerade erstellt haben.
4. Klicken Sie auf das Kontrollkästchen "Alle aktivieren". Senden und bestätigen Sie die Änderungen.

Schlussfolgerung

Zusammenfassend haben wir die erforderlichen Schritte gezeigt, um eine Cisco E-Mail Security Appliance für den Versand einer verschlüsselten E-Mail vorzubereiten:

1. Aktivieren von Cisco IronPort Email Encryption
2. Registrieren Sie Ihre ESA(s) und Ihre Organisation mit RES
3. Erstellen von Verschlüsselungsprofilen
4. Aktivieren von DLP

5. DLP-Nachrichtenaktionen werden erstellt
6. Erstellen von SvD-Policys
7. Anwenden von SvD-Policys auf eine ausgehende E-Mail-Policy

Weitere Informationen zu Ihrer ESA-Softwareversion finden Sie im ESA-Benutzerhandbuch. Benutzerhandbücher finden Sie unter dem folgenden Link:

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

Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.