

데이터 유출 방지 및 암호화 모범 사례 가이드

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[데이터 유출 방지 및 암호화 모범 사례에 대한 모범 사례 가이드](#)

[1. ESA에서 Cisco IronPort Email Encryption 활성화](#)

[2. ESA 및 조직을 RES에 등록](#)

[3. ESA에서 암호화 프로파일 생성](#)

[4. DLP\(Data Loss Prevention\) 활성화](#)

[5. 데이터 유출 방지 메시지 작업 생성](#)

[6. 데이터 유출 방지 정책 수립](#)

[7. 발신 이메일 정책에 DLP 정책 적용](#)

[결론](#)

[관련 정보](#)

소개

이 문서에서는 Cisco Email Security의 DLP(Data Loss Prevention) 및 암호화 모범 사례를 설명합니다.

이 문서에서는 Cisco ESA(Email Security Appliance) 및 클라우드 기반 Cisco RES(Registered Envelope Service)를 사용한 메시지 암호화 설정에 대해 설명합니다. 고객은 콘텐츠 필터링 및 DLP를 비롯한 다양한 유형의 정책을 사용하여 메시지 암호화를 사용하여 공용 인터넷을 통해 개별 메시지를 안전하게 전송할 수 있습니다. 이러한 정책의 생성은 이 시리즈 내의 다른 문서에서 논의됩니다. 이 문서에서는 정책이 암호화를 작업으로 사용할 수 있도록 ESA에서 암호화된 메일을 전송할 준비를 하는 데 중점을 둡니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문서에서는 다음 단계에 대해 설명합니다.

1. Cisco IronPort 이메일 암호화 활성화
2. RES에 ESA 및 조직 등록
3. 암호화 프로파일 생성
4. DLP 활성화
5. DLP 메시지 작업 생성
6. DLP 정책 생성
7. 발신 이메일 정책에 DLP 정책 적용

이러한 단계가 성공적으로 완료되면 ESA 관리자는 암호화를 작업으로 사용할 정책을 생성할 수 있습니다.

Cisco IronPort Email Encryption은 RES 암호화라고도 합니다. RES는 Cisco 클라우드의 "주요 서버"에 사용하는 이름입니다. RES 암호화 솔루션은 대칭 키 암호화를 사용합니다. 이는 메시지 암호화에 사용된 키가 메시지 해독에 사용된 키와 같음을 의미합니다. 암호화된 모든 메시지는 고유한 키를 사용하여 발신자가 메시지를 전송한 후(예: 수신자가 더 이상 메시지를 열 수 없도록 잠금 또는 만료) 메시지를 세부적으로 제어할 수 있습니다. 메시지를 암호화할 때, ESA는 암호화된 각 메시지에 대한 CRES에 암호화 키 및 메타데이터를 저장한다.

ESA는 "플러그"(예: 제목 콘텐츠), 콘텐츠 필터 매칭, DLP 정책 등 다양한 방법으로 메시지를 암호화하기로 결정할 수 있습니다. ESA가 메시지를 암호화하기로 결정하면 "Security Services(보안 서비스) > Cisco IronPort Email Encryption(Cisco IronPort 이메일 암호화)"에 지정된 "암호화 프로파일"(이메일 암호화 프로파일)을 사용하여 암호화합니다. 기본적으로 암호화 프로파일은 없습니다. 이에 대해서는 3. 암호화 프로파일 생성에서 설명합니다.

데이터 유출 방지 및 암호화 모범 사례에 대한 모범 사례 가이드

1. ESA에서 Cisco IronPort Email Encryption 활성화

 참고: 클러스터에 여러 ESA가 있는 경우 일반적으로 클러스터 레벨에서 관리되므로 #1단계 단계는 한 번만 수행하면 됩니다. 클러스터링되지 않은 시스템이 여러 개 있거나 시스템 레벨에서 이러한 설정을 관리하는 경우 각 ESA에서 #1단계를 수행해야 합니다.

1. ESA UI에서 Security Services(보안 서비스) > Cisco IronPort Email Encryption으로 이동합니다.
2. Cisco IronPort Email Encryption을 활성화하려면 확인란을 선택합니다.
3. EULA(End User License Agreement), Cisco IronPort Email Encryption 라이선스 계약에 동의합니다.
4. Email Encryption Global Settings(이메일 암호화 전역 설정)에서 Edit Settings(설정 편집)...를

클릭합니다.

- 어카운트의 기본 RES 관리자인 관리자/개인의 이메일 주소를 지정합니다. 이 이메일 계정은 회사의 RES 환경 관리와 연결됩니다.
- 선택 사항: 암호화할 기본 최대 메시지 크기는 10M입니다. 원하신다면 이 때 크기를 늘리거나 줄이셔도 됩니다.
- 선택 사항: ESA가 HTTPS를 통해 RES에 연결하기 위해 거쳐야 할 프록시가 있는 경우, 프록시를 통해 이를 허용하는 데 필요한 프록시 및 인증 설정을 추가합니다.

5. 컨피그레이션 변경 사항을 제출하고 커밋합니다.

이때 "Email Encryption Global Settings(이메일 암호화 전역 설정)"가 이와 같이 설정되었지만 아직 나열된 프로필이 없는 것을 볼 수 있습니다.

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. ESA 및 조직을 RES에 등록

#2단계는 주로 ESA 관리 콘솔 외부에서 수행됩니다.

 참고: ESA 등록 정보는 다음 TechNote에도 있습니다. [Cisco RES: 가상, 호스트 및 하드웨어 ESA 컨피그레이션의 어카운트 프로비저닝 예](#)

RES로 직접 이메일을 보내십시오. stg-cres-provisioning@cisco.com입니다.

ESA의 암호화 프로필에 대한 CRES 계정을 프로비저닝하려면 다음 정보를 제공하십시오.

1. 어카운트 이름(회사 이름을 정확히 기재하십시오. 나열해야 합니다.)
 1. CES(Cloud Email Security)/호스팅된 고객 계정의 경우 계정 이름이 "<Account Name> HOSTED"로 끝나도록 표시하십시오.
2. 계정 관리자에 사용할 이메일 주소(해당 관리자 이메일 주소를 지정하십시오.)

3. 전체 어플라이언스 일련 번호

1. 어플라이언스 일련 번호는 'version' 명령을 통해 ESA GUI(System Administration(시스템 관리) > Feature Keys(기능 키)) 또는 ESA CLI에서 찾을 수 있습니다. CRES 어카운트 관리를 위해 전체 어플라이언스 일련 번호가 필요하므로 VLN(가상 라이선스 번호) 또는 PAK(Product Activation Key) 라이선스를 제공할 수 없습니다.

4. 관리를 위해 CRES 계정에 매핑해야 하는 도메인 이름

참고: 이미 CRES 어카운트가 있는 경우 회사 이름 또는 기존 CRES 어카운트 번호를 입력하십시오. 그러면 새 어플라이언스 일련 번호가 올바른 어카운트에 추가되고 회사 정보 및 프로비저닝의 중복이 방지됩니다.

CRES 계정 프로비저닝과 관련하여 이메일을 보내는 경우 영업일 기준 1일로 응답하겠습니다. 즉, 각적인 지원 및 지원이 필요한 경우 Cisco TAC에 지원 요청을 접수하십시오. 이 작업은 Support Case Manager(<https://mycase.cloudapps.cisco.com/case>)를 통해 수행하거나 전화(<https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html>)로 [문의할](#) 수 있습니다.

 참고: 이 요청을 이메일로 보낸 후, 회사 RES 어카운트가 생성되고(아직 생성되지 않은 경우) S/N이 추가되는 데 하루가 걸릴 수 있습니다. #3단계의 "Provision(프로비저닝)" 작업은 완료될 때까지 작동하지 않습니다.

3. ESA에서 암호화 프로파일 생성

 참고: 클러스터에 여러 ESA가 있는 경우 일반적으로 클러스터 레벨에서 관리되므로 #1단계 단계는 한 번만 수행하면 됩니다. 클러스터링되지 않은 시스템이 여러 개 있거나 시스템 레벨에서 이러한 설정을 관리하는 경우 각 ESA에서 #1단계를 수행해야 합니다.

암호화 프로파일은 암호화된 메시지를 전송하는 방법을 지정합니다. 예를 들어, 조직은 매우 민감한 데이터를 자주 전송할 것임을 알고 있는 수신자의 한 부문에 대해 높은 보안 엔벨로프를 전송해야 할 수 있습니다. 동일한 조직은 수신자 커뮤니티의 다른 부문을 포함할 수 있는데, 이들은 덜 민감한 정보를 수신하고, 암호화된 메일을 수신하기 위해 사용자 ID와 비밀번호를 제공해야 하는 환자도 줄어들 수 있습니다. 이러한 수신자는 보안 수준이 낮은 봉투(Low-Security Envelope)에 적합합니다. 암호화 프로파일이 여러 개인 경우 암호화된 메시지 형식을 대상에 맞게 조정할 수 있습니다. 반면, 하나의 암호화 프로파일만으로도 많은 조직이 적합할 수 있습니다.

이 문서에서는 "CRES_HIGH", "CRES_MED" 및 "CRES_LOW"라는 세 가지 암호화 프로파일을 생성하는 예를 보여 줍니다.

1. ESA UI에서 Security Services(보안 서비스) > Cisco IronPort Email Encryption으로 이동합니다.
2. "Add Encryption Profile...(암호화 프로파일 추가...)"을 클릭합니다.
3. Encryption Profile(암호화 프로파일) 메뉴가 열리고 첫 번째 암호화 프로파일의 이름을 "CRES_HIGH"로 지정할 수 있습니다.
4. 봉투 메시지 보안을 아직 선택하지 않은 경우 "높은 보안"을 선택합니다.

5. 이 프로파일을 저장하려면 Submit(제출)을 클릭합니다.

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 Recipient must enter a passphrase to open the encrypted message, even if credentials are cached ("Remember Me" selected). ☐ Medium Security No passphrase entry required if recipient credentials are cached ("Remember Me" selected). ☐ No Passphrase Required The recipient does not need a passphrase to open the encrypted message.
Logo Link:	☒ No link ☐ Custom link URL: By defining a URL, the logo in the upper left corner of the recipient envelope will become a link (example: http://www.mycompany.com/).
Read Receipts:	☒ Enable Read Receipts 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 (see Mail Policies > Text Resources > Encryption Notification Template - HTML)
Encrypted Message Text Notification:	System Generated Preview Message (see Mail Policies > Text Resources > Encryption Notification Template - Text)
Encryption Failure Notification:	Message Subject: [ENCRYPTION FAILURE] Message Body: System Generated Preview Message (see Mail Policies > Text Resources > DSN Bounce and Encryption Failure Notification Template)
File name of the envelope attached to the encryption notification:	securedoc_\$(date)T\$(time).html

그런 다음 2-5단계를 반복하여 "CRES_MED" 및 "CRES_LOW"를 생성합니다. 각 프로파일에 대한 봉투 메시지 보안의 라디오 버튼을 변경하면 됩니다.

- CRES_HIGH 프로파일의 경우 "High Security" 라디오 버튼을 선택합니다.
- CRES_MED 프로파일의 경우 "Medium Security(중간 보안)" 라디오 버튼을 선택합니다.
- CRES_LOW 프로파일의 경우 "No Password Required" 라디오 버튼을 선택합니다

Enable Read Receipts(읽음 확인 활성화), Enable Secure Reply All(모두 보안 회신 활성화) 및 Enable Secure Message Forwarding(보안 메시지 전달 활성화) 옵션이 있습니다. Envelope Settings(봉투 설정)에서 "Advanced(고급)" 링크를 클릭하면 세 가지 대칭 암호화 알고리즘 중 하나를 선택할 수 있으며, Java 암호화 애플릿 없이 봉투를 전송하도록 지정할 수도 있습니다.

Envelope Settings(봉투 설정) 오른쪽에는 "Example Message(메시지 예)" 하이퍼텍스트 링크가 표시됩니다. 클릭하면 수신자가 HTML 첨부 파일을 연 후 이메일에 표시되는 보안 메시지 봉투(Secure Message Envelope)의 예가 표시됩니다.

Read Receipts(읽음 확인)는 수신자가 보안 메시지를 열면 암호화된 메시지의 발신자가 CRES로부터 이메일을 수신함을 의미합니다(수신자가 대칭 키를 내리고 메시지를 해독했음을 의미함).

Message Settings(메시지 설정) 오른쪽에는 "Example Message(메시지 예)" 하이퍼텍스트 링크가 표시됩니다. 클릭하면 열린 메시지가 어떻게 표시되는지, 즉 수신자가 봉투에 필요한 정보를 제공하고 암호화된 메시지를 열면 어떤 메시지가 표시되는지 표시됩니다.

Submit and commit changes(제출 및 커밋)를 클릭해야 합니다.

그러면 테이블의 행에 "Provision(프로비저닝)" 버튼이 표시됩니다. Provision(프로비저닝) 버튼은 Commit(커밋) 변경이 있을 때까지 표시되지 않습니다.

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		

Provision(프로비저닝) 버튼을 다시 클릭합니다. 회사 RES 어카운트가 생성되고 어플라이언스 S/N이 어카운트에 추가된 후에만 작동합니다. RES 어카운트가 ESA에 연결된 경우 프로비저닝 프로세스가 비교적 빠르게 수행됩니다. 그렇지 않은 경우 해당 프로세스를 먼저 완료해야 합니다.

프로비저닝이 완료되면 Cisco IronPort Email Encryption 페이지에 프로필이 프로비저닝된 것으로 표시됩니다.

4. DLP(Data Loss Prevention) 활성화

1. ESA UI에서 Security Services(보안 서비스) > Data Loss Prevention(데이터 손실 방지)으로 이동합니다.
2. Enable...을 클릭하여 DLP를 활성화합니다.
3. EULA, Data Loss Prevention 라이선스 계약에 동의합니다.
4. Enable matched content logging(일치하는 콘텐츠 로깅 활성화) 확인란을 클릭합니다.

5. Enable automatic updates(자동 업데이트 활성화) 확인란을 클릭합니다.
6. Submit(제출)을 클릭합니다.

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

어플라이언스에서 DLP 엔진 및 사전 정의된 콘텐츠 일치 분류자에 대한 업데이트는 다른 보안 서비스에 대한 업데이트와 무관합니다. 3~5분의 정기 Talos 서명 업데이트는 서로 다르며 DLP 정책 및 사전 업데이트를 포함하지 않습니다. 여기서 업데이트를 활성화해야 합니다.

"Matched Content Logging(일치하는 콘텐츠 로깅)"이 활성화된 경우, 메시지 추적은 위반을 일으킨 이메일 콘텐츠를 표시할 수 있습니다. 다음은 DLP 위반의 원인이 된 이메일 콘텐츠를 보여 주는 메시지 추적의 예입니다. 이러한 방식으로 관리자는 어떤 데이터가 특정 DLP 정책을 트리거했는지 정확하게 알 수 있습니다.

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 540410R95RA54RR1 110 R/2009

데이터 유출 방지

위반

5. 데이터 유출 방지 메시지 작업 생성

DLP 격리 생성

DLP 정책을 위반하는 메시지의 복사본을 유지하려는 경우 각 정책 위반 유형에 대해 개별 정책 격리를 생성할 수 있습니다. 이는 DLP 정책을 위반하는 아웃바운드 메시지가 기록되고 전달되지만 메시지에 대한 작업은 수행되지 않는 '투명' POV를 실행할 때 특히 유용합니다.

1. SMA에서 Email(이메일) > Message Quarantine(메시지 격리) > Policy, Virus, and Outbreak Quarantines(정책, 바이러스 및 Outbreak 격리)로 이동합니다

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	

2. 시작하기 전 격리 테이블은 이렇게 보입니다:
정책 바이러스 및 Outbreak 격리

3. "Add Policy Quarantine(정책 격리 추가)" 버튼을 클릭하고 DLP 정책에서 사용할 격리를 생성합니다.

다음은 중간 DLP 위반에 대한 격리 예입니다. 격리를 분할할 수 있으며 여러 DLP 규칙에 대해 필요할 수 있습니다.

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

DLP 퀴런틴 예

DLP 메시지 작업 정보

DLP 메시지 작업은 발신 이메일에서 DLP 위반을 탐지할 때 ESA가 수행할 작업에 대해 설명합니다. 기본 및 보조 DLP 작업을 지정할 수 있으며, 서로 다른 위반 유형 및 심각도에 대해 서로 다른 작업을 할당할 수 있습니다.

주요 작업은 다음과 같습니다.

- 제공
- 삭제
- 격리

DLP 위반이 기록되고 보고되지만 메시지가 정지/격리 또는 암호화되지 않는 읽기 전용 상태의 경우 Deliver 작업이 가장 자주 사용됩니다.

보조 작업은 다음과 같습니다.

- 사용자 지정 격리 또는 '정책' 격리로 사본 발송
- 메시지를 암호화합니다. 어플라이언스는 메시지 본문만 암호화합니다. 메시지 헤더를 암호화하지 않습니다.
- Subject 헤더 변경.
- 메시지에 면책조항 텍스트/HTML을 추가합니다.
- 메시지를 대체 대상 메일 호스트로 보내는 중입니다.
- 메시지의 숨은 참조 복사본을 보내는 중입니다.
- 발신자 및/또는 기타 연락처에 DLP 위반 알림을 보내는 중입니다.

이러한 작업은 상호 배타적이지 않습니다. 서로 다른 사용자 그룹에 대한 다양한 처리 요구에 따라 서로 다른 DLP 정책 내에서 일부 작업을 결합할 수 있습니다.

다음 DLP 작업을 구현합니다. 암호화

이러한 작업에서는 ESA에서 암호화 라이선스가 부여되고 구성되며 이전 섹션에서 수행한 것과 같이 높은 보안, 중간 보안 및 낮은 보안을 위해 3개의 프로파일이 생성된 것으로 가정합니다.

- CRES_높음
- CRES_메드
- CRES_낮음

DLP 메시지 작업 생성

1. Mail Policies(메일 정책) > DLP Message Customizations(DLP 메시지 사용자 맞춤화)로 이동합니다.
2. "Add Message Action(메시지 작업 추가)" 버튼을 클릭하고 다음 DLP 작업을 추가합니다. 메시지 작업을 제출한 후 변경 사항을 커밋해야 합니다.

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

메시지 작업

6. 데이터 유출 방지 정책 수립

DLP 정책에는 다음이 포함됩니다.

- 발신 메시지에 민감한 데이터가 포함되어 있는지 여부를 결정하는 조건 집합
- 메시지에 이러한 데이터가 포함된 경우 수행할 작업.

1. Mail Policies(메일 정책) > DLP Policy Manager(DLP 정책 관리자)로 이동합니다.
2. 'Add DLP Policy'(DLP 정책 추가)를 클릭합니다.
3. "Regulatory Compliance(규정 준수)" 공개 삼각형을 엽니다.

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) Customization recommended.
Add	US GLBA (Gramm Leach Bliley Act) Customization recommended.
Add	US HIPAA and HITECH Customization recommended.
Add	US HIPAA and HITECH (Low Threshold) Customization recommended.
Add	US SOX (Sarbanes Oxley)
▶ US State Regulatory Compliance	
▶ Acceptable Use	
▶ Privacy Protection	
▶ Intellectual Property Protection	
▶ Company Confidential	
▶ Custom Policy	

« Back

DLP 정책 템플릿

4. PCI 정책의 경우 PCI-DSS 왼쪽에 있는 "Add(추가)" 버튼을 클릭합니다.

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><tr><td>IGNORE</td><td>LOW</td><td>MEDIUM</td><td>HIGH</td><td>CRITICAL</td></tr><tr><td>0 - 14</td><td>15 - 52</td><td>53 - 72</td><td>73 - 87</td><td>88 - 100</td></tr></table> <a>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 DLP 규칙의 예

5. Critical Severity Incident에서 이전에 구성한 "Encrypt Medium and Deliver" 작업을 선택합니다. 심각도가 낮은 인시던트는 변경할 수 있지만, 지금은 심각도가 높은 인시던트를 상속받도록 합니다. 변경 사항을 제출한 다음 커밋합니다.

7. 발신 이메일 정책에 DLP 정책 적용

1. 다음으로 이동합니다. Mail Policies(메일 정책) > Outgoing Mail Policies(발신 메일 정책)
2. Default Policy(기본 정책)에 대한 DLP의 제어 셀을 클릭합니다. 아직 활성화하지 않은 경우

"Disabled(비활성화됨)"로 표시됩니다.

3. Disable DLP(DLP 비활성화)에서 Enable DLP(DLP 활성화)로 폴다운 버튼을 변경하면 방금 생성한 DLP 정책이 즉시 표시됩니다.
4. "Enable All(모두 활성화)" 확인란을 클릭합니다. 변경 사항을 제출한 다음 커밋합니다.

결론

요약하면, 암호화된 이메일을 전송하기 위해 Cisco Email Security Appliance를 준비하는 데 필요한 단계를 보여드렸습니다.

1. Cisco IronPort 이메일 암호화 활성화
2. RES에 ESA 및 조직 등록
3. 암호화 프로파일 생성
4. DLP 활성화
5. DLP 메시지 작업 생성
6. DLP 정책 생성
7. 발신 이메일 정책에 DLP 정책 적용

자세한 내용은 ESA 소프트웨어 릴리스에 해당하는 ESA 사용 설명서를 참조하십시오. 사용 설명서는 다음 링크에서 확인할 수 있습니다.

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

관련 정보

- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.