수신 및 발신 콘텐츠 필터에 대한 모범 사례 가이드

목차

소개

Content Filters(콘텐츠 필터)를 사용하면 이메일의 복잡한 세부 정보를 검사하고 이메일에 대해 Action(작업 없음)을 수행할 수 있습니다.수신 또는 발신 콘텐츠 필터가 생성되면 수신 또는 발신 메일 정책에 적용합니다.이메일이 콘텐츠 필터와 일치하면 Cisco ESA(Email Security Appliance) 및 SMA(Security Management Appliance)의 "Content Filters" 보고서에서 콘텐츠 필터와 일치하는 모든 이메일을 볼 수 있습니다.따라서 아무 조치도 취하지 않더라도 조직에 들어오고 나가는 이메일 유형에 대한 중요한 정보를 확보하여 이메일 흐름을 "패턴"으로 설정할 수 있습니다.

다양한 콘텐츠 필터 "Conditions(조건)" 및 "Actions(작업)"가 있으므로 이 문서에서는 매우 일반적이며 권장되는 수신 및 발신 콘텐츠 필터를 단계별로 안내합니다.

단계 개요

1단계:필요한 사전 가져오기

이 문서에서는 일부 Best Practices Incoming 및 Outgoing Content Filters를 구현하는 데 필요한 단계를 제공합니다.작성하려는 콘텐츠 필터는 몇 개의 사전을 참조하므로 먼저 해당 사전을 가져와야 합니다.ESA는 사전과 함께 제공되며, 생성할 콘텐츠 필터에서 해당 사전을 참조하기 위해 해당 사전을 컨피그레이션으로 가져오기만 하면 됩니다.

2단계: 중앙 집중식 격리 생성

대부분의 콘텐츠 필터에서 "Action(작업)"을 설정하여 이메일(또는 이메일 사본)을 지정된 맞춤형(새로운) 격리로 격리합니다. 따라서 먼저 SMA에 이러한 격리를 생성해야 합니다. 이 문서에서는 ESA와 SMA 간에 중앙 집중식 PVO(정책, 바이러스 및 Outbreak) 격리를 활성화했다고 가정합니다.

3단계:수신 및 발신 콘텐츠 필터 생성 및 정책에 적용

사전을 가져오고 격리가 생성되면 인바운드 콘텐츠 필터를 생성하고 이를 수신 메일 정책에 적용한 다음 발신 콘텐츠 필터를 생성하여 발신 메일 정책에 적용합니다.

1단계:필요한 사전 가져오기

컨텐트 필터에서 참조할 사전 가져오기:

- ESA 어플라이언스에서 **"Mail Policies > Dictionaries"로 이동합니다.**
- 페이지 오른쪽의 "**Import Dictionary**(사전 가져오기)" 버튼을 클릭합니다.

욕설:

- **"IronPort 어플라이언스의 configuration 디렉토리에서 가져오기"를 선택합니다.**
- "**annique.txt**"를 선택하고 "**Next**"를 클릭합니다.
- 이름: **불경한**
- **"단어 전체 일치"**(매우 중요)
- 용어 수정(새 용어 추가 또는 원치 않는 용어 제거)
- "Submit(제출)**"을 클릭합니다.**

성적 내용:

- **"IronPort 어플라이언스의 configuration 디렉토리에서 가져오기"를 선택합니다.**
- "**성적_content.txt**"를 선택하고 "**Next**"를 클릭합니다.
- Name(이름): **G성적 내용**
- **"단어 전체 일치"**(매우 중요)
- 용어 수정(새 용어 추가 또는 원치 않는 용어 제거)
- "Submit(제출)**"을 클릭합니다.**

독점:

- **"IronPort 어플라이언스의 configuration 디렉토리에서 가져오기"를 선택합니다.**
- "**proprietary_content.txt**"를 선택하고 "**Next**"를 클릭합니다.
- 이름: **독점**
- **"단어 전체 일치"**(매우 중요)
- 용어 수정(새 용어 추가 또는 원치 않는 용어 제거)
- **"Submit(제출)"을 클릭합니다.**

2단계:중앙 집중식 격리 생성

- SMA에서 **"Email Tab(이메일 탭) > Message Quarantine(메시지 격리) > PVO Quarantines(PVO 격리)"로 이동합니다.**
- 이것이 시작하기 전에 Quarantines(격리) 테이블의 모양입니다.모든 격리는 기본값입니다.

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	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

- 다음을 클릭합니다. **"정책 격리 추가..."** 단추
- 아래 격리를 생성합니다.

- 일부는 수신 콘텐츠 필터에서 사용되며 일부는 발신 콘텐츠 필터에서 사용됩니다.동일한 방식으로 생성합니다.

PVO 격리 - 수신 콘텐츠 필터에서 사용

URL 악성 인바운드:
이름:URL 악성 인바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

URL 범주 인바운드:
이름:URL 범주 인바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

은행 데이터 인바운드:
이름:은행 데이터 인바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

SSN 인바운드:
이름:SSN 인바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

부적절한 인바운드:
이름:부적절한 인바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

SPF 하드 실패:
이름:SPF 하드 실패
보존 기간:14일
기본 작업:삭제
여유 공간:사용

SPF 소프트 실패:
이름:SPF 소프트 실패
보존 기간:14일
기본 작업:삭제
여유 공간:사용

스푸프메일:
이름:스푸프메일
보존 기간:14일
기본 작업:삭제
여유 공간:사용

DKIM 하드 실패:
이름:DKIM 하드 실패
보존 기간:14일
기본 작업:삭제
여유 공간:사용

암호로 보호된 인바운드:
이름:Pwd 보호 인바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

PVO 격리 - 발신 콘텐츠 필터에서 사용

은행 데이터 아웃바운드:
이름:은행 데이터 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

SSN 아웃바운드:
이름:SSN 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

부적절한 아웃바운드:
이름:부적절한 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

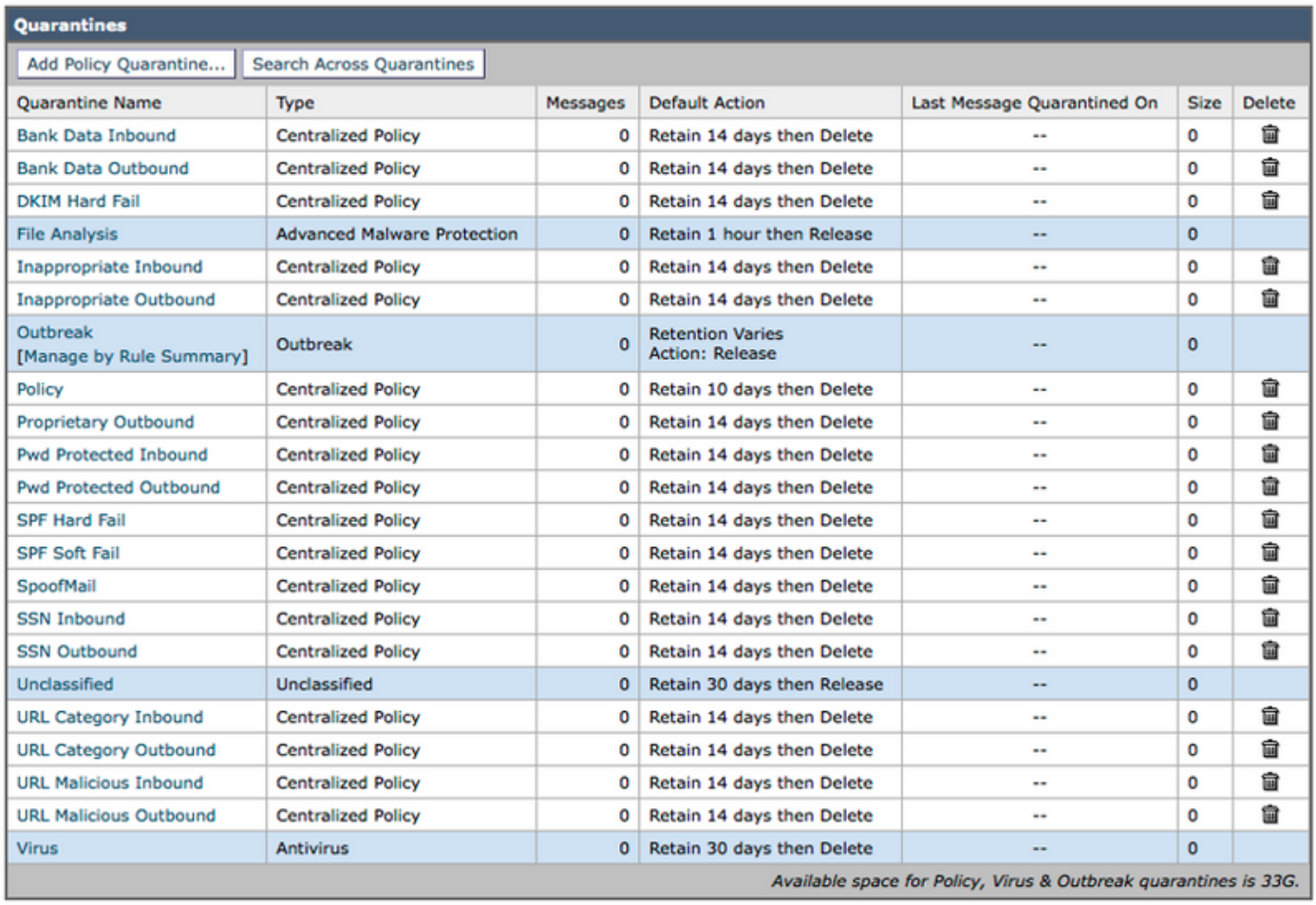
독점 아웃바운드:
이름:독점 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

URL 악성 아웃바운드:
이름:URL 악성 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

URL 범주 아웃바운드:
이름:URL 범주 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

암호로 보호된 아웃바운드:
이름:Pwd 보호된 아웃바운드
보존 기간:14일
기본 작업:삭제
여유 공간:사용

- 다음은 모든 PVO 격리를 생성한 후 PVO 테이블을 어떻게 살펴보는지 보여줍니다.



Quarantines

Add Policy Quarantine... | Search Across Quarantines

Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
Bank Data Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Bank Data Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
DKIM Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Inappropriate Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Inappropriate Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Proprietary Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Pwd Protected Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Hard Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SPF Soft Fail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SpoofMail	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
SSN Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
URL Category Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Category Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Inbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
URL Malicious Outbound	Centralized Policy	0	Retain 14 days then Delete	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

3단계:수신 콘텐츠 필터 생성

사전을 가져오고 PVO 격리가 생성되면 이제 수신 콘텐츠 필터 생성을 시작할 수 있습니다.

- "Mail **Policies(메일 정책) > Incoming Content Filters(수신 콘텐츠 필터)"로 이동합니다.**
- 생성해야 하는 수신 콘텐츠 필터 테이블이 있습니다.예를 들어, 표 아래에는 첫 번째 항목을 만드는 방법을 보여주는 스크린샷이 있습니다.

수신 콘텐츠 필터 만들기

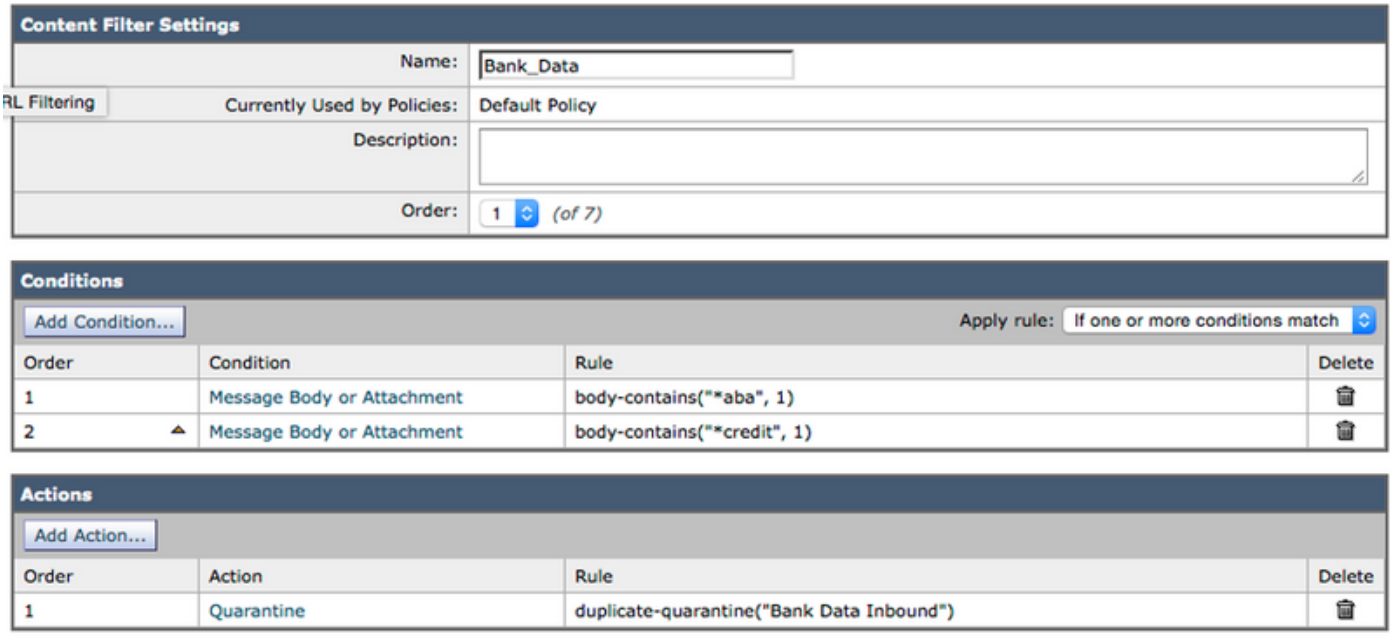
이름:**은행_데이터**
2가지 조건 추가:
  메시지 본문 또는 첨부 파일:
    스마트 식별자 포함:ABA 라우팅 번호
    스마트 식별자 포함:신용 카드 번호
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"은행 데이터 인바운드(중앙 집중식)"
    중복된 메시지:사용
(적용 규칙은 "하나 이상의 조건이 일치하는 경우"여야 합니다.)
이름:**SSN**
조건 하나 추가:
  메시지 본문 또는 첨부 파일:
    스마트 식별자 포함:사회 보장 번호(SSN)
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"SSN 인바운드(중앙 집중식)"
    중복된 메시지:사용

이름:**부적절한**
2가지 조건 추가:
  메시지 본문 또는 첨부 파일:
    사전에 용어 포함:욕설
    사전에 용어 포함:성적_내용
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"부적절한 인바운드(중앙 집중식)"
    중복된 메시지:사용
이름:**URL_범주**
조건 하나 추가:
  URL 범주:
    범주 선택:
      성인, 데이트, 필터 회피, 프리웨어 및 셰어웨어, 도박,
      게임, 해킹, 란제리 그리고 수영복, 비성적인 나체,
      파크된 도메인, 피어 파일 전송, 포르노그라피
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"URL 범주 인바운드(중앙 집중식)"
    중복된 메시지:사용
(참고:이 콘텐츠 필터를 사용하려면 "보안 서비스"—> "URL 필터링"을 활성화해야 합니다.
이름:**URL_악성**
조건 하나 추가:
  URL 평판:
    URL 평판:악성(-10.0 ~ -6.0)
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"URL 악성 인바운드(중앙 집중식)"
    중복된 메시지:사용 안 함(**** 원본 격리 ***)
이름:**암호 보호**
조건 하나 추가:
  첨부 파일 보호:하나 이상의 첨부 파일이 보호됨
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"Pwd Protected Inbound(중앙 집중식)"
    중복된 메시지:사용
이름:**크기_10M**
조건 하나 추가:
  메시지 크기:
    다음보다 크거나 같음:1,000만
하나의 작업 추가:
  메시지 태그 추가:
    용어 입력:NOOP
(참고:어떤 작업이 있어야 하므로 여기서는 작업을 수행하지 않음을 나타내는 메시지를 "태그"로 지정합니다.콘텐츠 필터가 "Matched(일치)"인 경우 보고서에 표시될 수 있습니다.Reporting(보고)에 표시하려면 "작업"을 수행할 필요가 없습니다.)
이름:**SPF_Hard_Fail**
조건 하나 추가:
  SPF 확인:"is" 실패
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"SPF Hard Fail(중앙 집중식)"
    중복된 메시지:사용

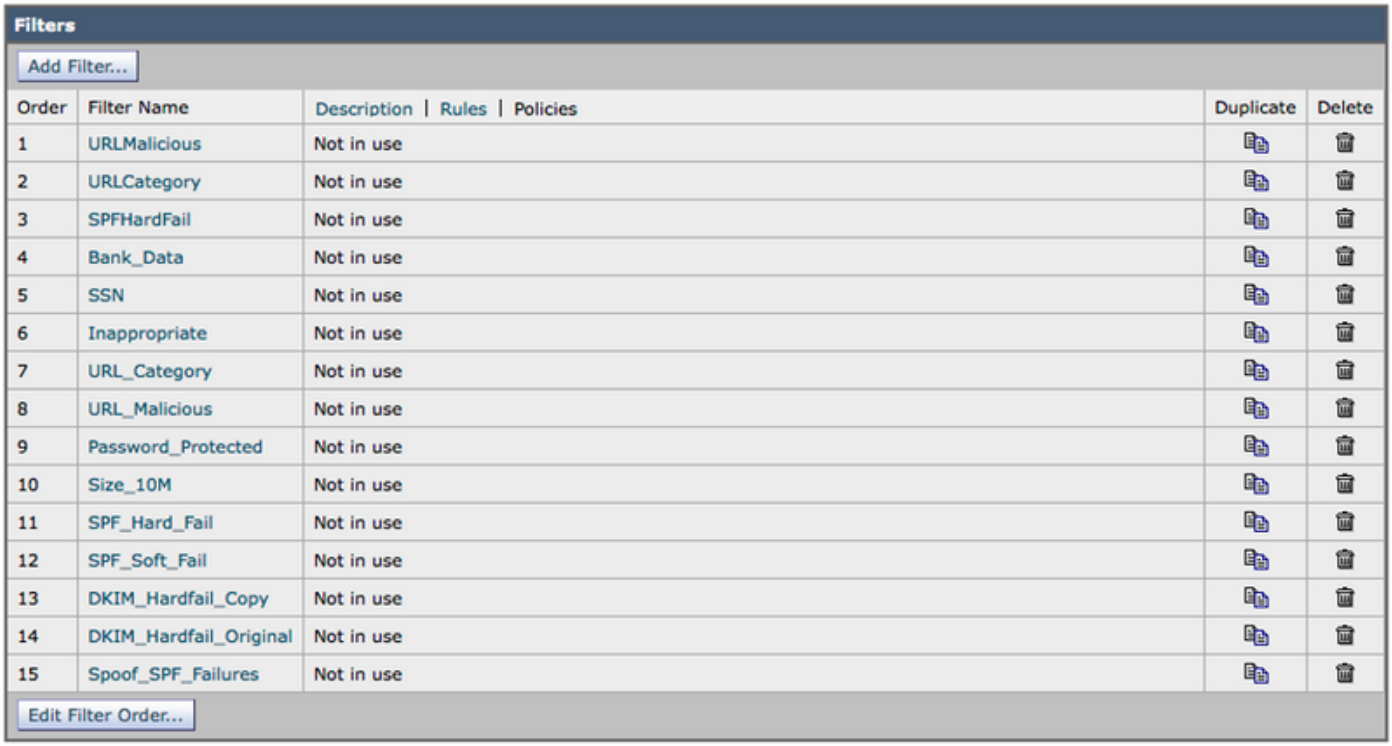
(참고:"is fail"은 Hard SPF 오류이며, 도메인 소유자가 SPF 레코드에 나열되지 않은 발신자로부터 받은 모든 이메일을 삭제하도록 지시하고 있음을 의미합니다.처음에는 "Duplicate message(중복 메시지)"를 사용하고 원래 메시지를 격리하기 전에 1~2주 동안 오류를 검토하는 것이 좋습니다(예: 중복 메시지 끄기).

이름:**SPF_Soft_Fail**
조건 하나 추가:
  SPF 확인:"is" 소프트페일
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"SPF Soft Fail(중앙 집중식)"
    중복된 메시지:사용
이름:**DKIM_Hardfail_Copy**
조건 하나 추가:
  DKIM 인증:"is" 하드웨어 장애
두 가지 작업 추가:
  헤더 추가/편집:
    헤더 이름:제목
    "Prepend to the Value of Existing Header"를 클릭하고 다음을 입력합니다.[복사 - 해제 안 함]"
  쿼런틴:
    쿼런틴으로 메시지 보내기:"DKIM Hard Fail(중앙 집중식)"
    중복된 메시지:사용
(참고:처음에 메시지의 복사본을 격리합니다.)
이름:**DKIM_하드페일_원본**
조건 하나 추가:
  DKIM 인증:"is" 하드웨어 장애
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"DKIM Hard Fail(중앙 집중식)"
    중복된 메시지:사용 안 함
(참고:PayPal 및 eBay 도메인에 대한 또 다른 수신 메일 정책 행을 만들고 DKIM 확인을 통과해야 하는 도메인에 대해 이 콘텐츠 필터를 사용합니다.)
이름:**Spoof_SPF_Failures**
하나의 조건을 추가하지만 SOFTFAIL 및 Hardfail이 모두 선택되어 있습니다.
  SPF 확인:"is" Softfail을 클릭하고 "Fail"을 클릭합니다.
 "Softfail"과 "Fail"을 클릭한 두 개의 확인란
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"SpoofMail(중앙 집중식)"
    중복된 메시지:사용
(참고:이 콘텐츠 필터를 사용하여 자신의 도메인에서 보내는 것처럼 가장하는 수신 이메일의 스푸핑 작업을 수행합니다.먼저 사본을 격리하기 위한 작업 집합으로 시작하고 SpoofMail 격리를 2주 검토한 후 SPF TXT DNS 레코드를 수정하여 모든 합법적인 발신자를 추가할 수 있으며, 경우에 따라 중복 메시지 확인란을 비활성화하여 이 콘텐츠 필터를 변경하여 원본을 격리할 수 있습니다.)

예를 들어, Bank_Data Content Filter는 제출하기 전에 다음과 같이 표시되어야 합니다.



모든 수신 컨텐트 필터를 만든 다음 테이블은 다음과 같습니다.



"Policies" 기능이 선택되었으므로(맨 위 중간에 Policies 하이퍼텍스트 표시) 중간 열에는 콘텐츠 필터가 적용된 수신 메일 정책이 표시됩니다.Incoming Mail Policy(수신 메일 정책)에 적용하지 않았으므로 "Not in use(사용 안 함)"가 표시됩니다.

수신 메일 정책에 수신 콘텐츠 필터 적용

- 다음으로 이동:**"메일 정책 > 수신 메일 정책"**
- Content Filters(콘텐츠 필터) 셀에서 **"Default Policy(기본 정책)"**에 대한 **"Disabled(비활성화됨)" 텍스트를 클릭합니다**.
- 풀다운 메뉴 버튼이 **"Disable Content Filters(콘텐츠 필터 비활성화)"로 설정됩니다**.
- 버튼을 클릭하고 **"Enable Content Filters(콘텐츠 필터 활성화)"로** 설정하면 생성된 모든 수신 콘텐츠 필터가 즉시 표시됩니다.

- DKIM_Hardfail_Original 및 Spoof_SPF_Failures를 제외한 모든 필터를 활성화합니다.
- **"제출"** 및 **"커밋"**.

eBay 및 Paypal용 DKIM 확인 및 도메인에 대한 Spoof Email 보호

이 두 주제에는 DKIM Verification 및 SPF Verification을 활용하는 콘텐츠 필터가 포함됩니다.따라서 먼저 DKIM 및 SPF Verification이 모두 활성화되었는지 확인해야 합니다.

1. 메일 플로우 정책에서 DKIM 및 SPF 확인을 활성화합니다.

- 다음으로 이동:**"메일 정책 > 메일 플로우 정책"**
- "Connection Behavior(연결 동작)"가 "Accept(수락)"인 모든 메일 흐름 정책에서 DKIM 및 SPF 확인을 활성화합니다.
- 하단 하이퍼텍스트 **"Default Policy Parameters(기본 정책 매개변수)"**를 클릭하고 **"DKIM Verification(DKIM 확인)"**을 **"On"** 및 **"SFP/SIDF Verification(SFP/SIDF 확인)을 "On"**으로 **설정합니다.**
- **"Submit(제출)"** 및 **"Commit(커밋)"을 클릭합니다**.
- 메일 플로우 정책 테이블이 표시됩니다.Behavior(동작)라는 열**을** 보고 Behavior(동작)가 **"Relay(릴레이)"**로 설정된 메일 플로우 정책을 수정합니다.
- 해당 **메일** 플로우 정책에 대해 DKIM 및 SPF 확인을 모두 "해제"합니다.
- **"Submit(제출)"** 및 **"Commit(커밋)"을 클릭합니다**.

아웃바운드 Exchange Mail Server에서 ESA로 수신되는 이메일에 대해 DKIM 또는 SPF 확인을 수행하지 않도록 ESA에서 합니다.대부분의 컨피그레이션에서는 "RELAYED" 메일 흐름 정책이 Behavior of Relay의 유일한 행입니다.

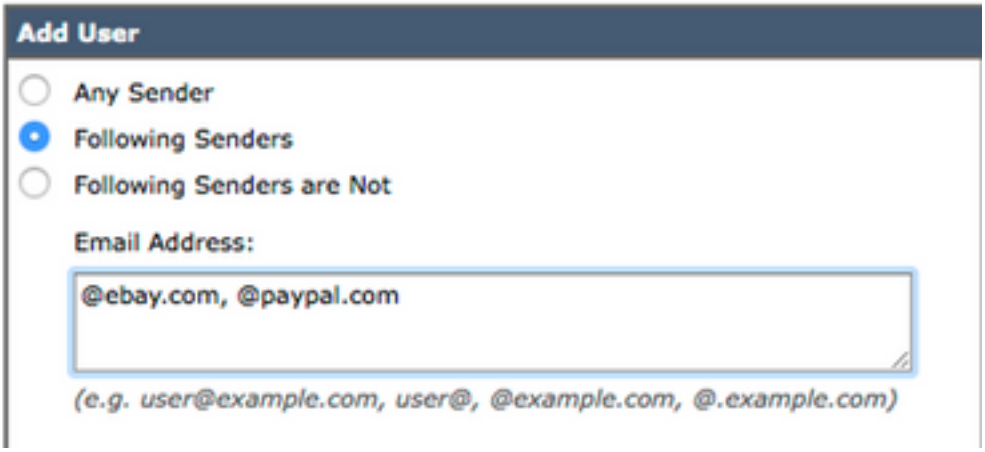
2. eBay 및 Paypal에 대한 새 수신 메일 플로우 정책 생성

eBay 및 Paypal에서 받은 인바운드 이메일은 항상 DKIM 확인을 통과해야 합니다.따라서 해당 도메인의 이메일에 DKIM_Hardfail_Original Inal Incoming Content Filter를 사용하도록 또 다른 수신 메일 정책을 생성합니다.

- 다음으로 이동:**"메일 정책 > 수신 메일 정책"**
- **"Add Policy" 버튼을 클릭합니다.**
- 이름 입력:**"DKIM 하드웨어 원본"**
- 다음을 클릭합니다. **"사용자 추가..."** 단추를 클릭합니다.

다음 컨피그레이션 패널에서는 이 새로운 수신 메일 정책과 매칭할 메시지를 정의할 수 있습니다 .발신자(컨피그레이션 패널의 왼쪽 부분)의 기준만 정의하겠습니다.

- 클릭 **"보낸 사람 팔로우"** 라디오 버튼을 클릭하고 Email Addresses 테이블에 **"@ebay.com, @paypal.com"**



- 다음을 클릭합니다. **"확인"** 단추를 클릭합니다.
- 클릭 **"제출"**.

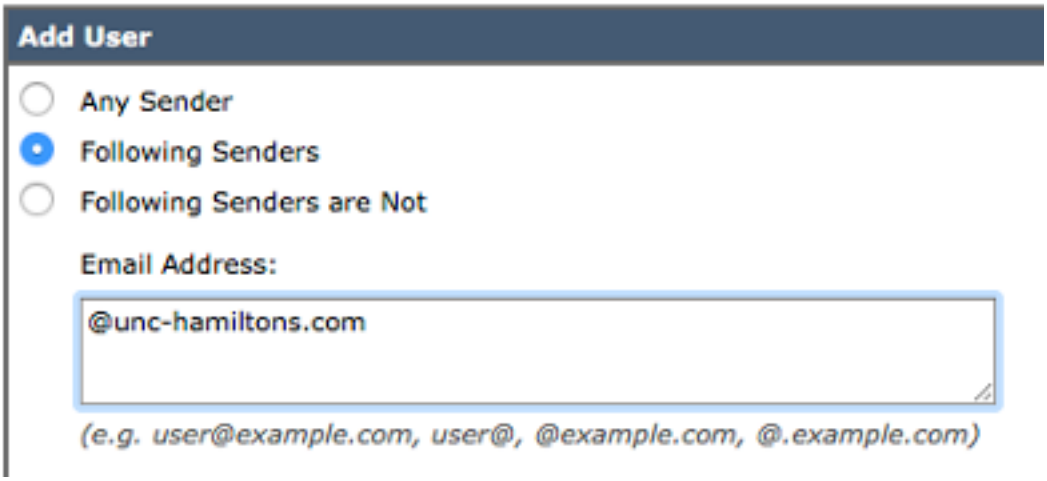
3. 도메인에 대한 새 수신 메일 플로우 정책 생성(스푸핑 보호)

이 섹션의 단계를 통해 자신의 도메인의 발신 이메일 주소가 있고 SPF 확인에 실패한 수신 이메일에 대한 조치를 취할 수 있습니다.물론 이는 DNS에 SPF Text Record를 이미 게시한 것에 의존합니다.도메인에 대한 SPF 텍스트 리소스 레코드를 생성/게시하지 않은 경우 이 단계를 건너뜁니다.

- 다음으로 이동:**"메일 정책 > 수신 메일 정책"**
- **"Add Policy" 버튼을 클릭합니다.**
- 이름 입력:**"spoof_Protection"**
- 다음을 클릭합니다. **"사용자 추가..."** 단추를 클릭합니다.

다음 컨피그레이션 패널에서는 이 새 수신 메일 정책 행과 매칭할 메시지를 정의할 수 있습니다.발신자(컨피그레이션 패널의 왼쪽 부분)에 대한 기준만 정의할 수 있습니다.

- 다음을 클릭합니다. **"보낸 사람 팔로우"** 라디오 버튼을 클릭한 다음 **"이메일 주소:"** 텍스트 상자에 도메인을 입력합니다.내 도메인은 **"@unc-hamilton.com"입니다.**



- 클릭 **"제출"**.

Incoming Mail Policies(수신 메일 정책) 테이블이 다시 표시되지만 이제 Default Policy(기본 정책) 위에 두 번째 새 Mail Policy(메일 정책) 행이 있습니다.

- 새 행에 **대한** Content Filters 셀에서 **(기본값 사용) 하이퍼텍스트**를 클릭합니다.
- 풀다운 메뉴를 **"Enable Content Filters (Customized Settings)"로 전환합니다**.
- "Spoof_**SPF_Failures"**를 확인하여 "DKIM_**Hardfail_Copy"** 및 **"DKIM_Hardfail_Original"**이 선택되지 않았는지 확인합니다.

- **"Submit(제출)"** 및 **"Commit changes(변경 사항 커밋)"를 클릭합니다.**

Incoming Mail Policies(수신 메일 정책) 테이블은 다음과 같습니다.

Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Delete
1	DKIM Hardfail Original	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	🗑
2	Spoof_Protection	(use default)	(use default)	(use default)	(use default)	URLMalicious URLCategory SPFHardFail Bank_Data ...	(use default)	🗑
	Default Policy	IronPort Intelligent Multi-Scan Positive: Quarantine Suspected: Quarantine	Sophos Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop	File Reputation Unscannable: Deliver Malware File: Drop Pending Analysis: Deliver	Disabled	URLMalicious URLCategory SPFHardFail Bank_Data ...	Retention Time: Virus: 1 day	

4단계:발송 컨텐트 필터 생성

- "Mail **Policies(메일 정책) > Outgoing Content Filters(발신 콘텐츠 필터)"로 이동합니다.**
- 생성해야 하는 발송 컨텐트 필터 테이블이 있습니다.

이러한 발신 콘텐츠 필터 만들기

이름:**은행_데이터**
2가지 조건 추가:
  메시지 본문 또는 첨부 파일:
    스마트 식별자 포함:ABA 라우팅 번호
    스마트 식별자 포함:신용 카드 번호
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"은행 데이터 아웃바운드(중앙 집중식)"
    중복된 메시지:사용
(적용 규칙은 "하나 이상의 조건이 일치하는 경우"여야 합니다.)
이름:**SSN**
조건 하나 추가:
  메시지 본문 또는 첨부 파일:
    스마트 식별자 포함:사회 보장 번호(SSN)
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"SSN 아웃바운드(중앙 집중식)"
    중복된 메시지: 사용
이름:**부적절한**
2가지 조건 추가:
  메시지 본문 또는 첨부 파일:
    사전에 용어 포함:욕설
    사전에 용어 포함:성적_내용
하나의 작업 추가:
  쿼런틴:
    쿼런틴으로 메시지 보내기:"부적절한 아웃바운드(중앙 집중식)"
    중복된 메시지:사용
이름:**URL_범주**
조건 하나 추가:
  URL 범주:
    범주 선택:
      성인, 데이트, 필터 회피, 프리웨어 및 셰어웨어, 도박,

게임, 해킹, 란제리 그리고 수영복, 비성적인 나체,
파크된 도메인, 피어 파일 전송, 포르노그라피
하나의 작업 추가:
쿼런틴:
쿼런틴으로 메시지 보내기:"URL 범주 아웃바운드(중앙 집중식)"
중복된 메시지:사용
이름:**URL_악성**
조건 하나 추가:
URL 평판:
URL 평판:악성(-10.0 ~ -6.0)
하나의 작업 추가:
쿼런틴:
쿼런틴으로 메시지 보내기:"URL 악성 아웃바운드(중앙 집중식)"
중복된 메시지:사용 안 함(**** 원본 격리 ***)
이름:**암호 보호**
조건 하나 추가:
첨부 파일 보호:하나 이상의 첨부 파일이 보호됨
하나의 작업 추가:
쿼런틴:
쿼런틴으로 메시지 보내기:"Pwd Protected Outbound(중앙 집중식)"
중복된 메시지:사용
이름:**크기_10M**
조건 하나 추가:
메시지 크기:
다음보다 크거나 같음:1,000만
하나의 작업 추가:
메시지 태그 추가:
용어 입력:NOOP
(참고:어떤 작업이 있어야 하므로 여기서는 작업을 수행하지 않음을 나타내는 메시지를 "태그"로 지정합니다.콘텐츠 필터가 "Matched(일치)"인 경우 보고서에 표시될 수 있습니다.Reporting(보고)에 표시하려면 "작업"을 수행할 필요가 없습니다.)
이름:**독점적**
조건 하나 추가:
메시지 본문 또는 첨부 파일:
사전에 용어 포함:독점적
하나의 작업 추가:
쿼런틴:
쿼런틴으로 메시지 보내기:"독점적(중앙 집중식)"
중복된 메시지:사용

"Policies(정책)" 기능이 선택되었으므로(맨 위 중간에 Policies(정책) 하이퍼텍스트가 표시됨) 중간 열에는 콘텐츠 필터가 적용된 발신 메일 정책이 표시됩니다.발송 메일 정책에 적용하지 않았으므로 "사용 안 함"이 표시됩니다.

- 다음으로 이동:**"메일 정책 > 발송 메일 정책"**
- Default Policy(기본 정책)**에** 대한 Content Filters(콘텐츠 필터) 셀에서 "Disabled(비활성화됨)" 텍스트를 클릭합니다.
- 풀다운 메뉴 버튼이 "**Disable Content Filters(콘텐츠 필터 비활성화**)"로 설정됩니다.
- 버튼을 클릭하고 **"Enable Content Filters(콘텐츠 필터 활성화)**"로 설정하면 생성된 모든 발신 콘텐츠 필터가 즉시 표시됩니다.
- **"**모든 필터 사용"
- **"제출"** 및 **"커밋"**.

요약

이제 수신 및 발신 콘텐츠 필터에 대한 초기 모범 사례를 구현했습니다.대부분의(전부는 아님) 콘텐츠 필터는 격리 조치를 사용하고 "중복된 메시지" 옵션을 확인(활성화)하도록 선택했습니다. 이 옵션은 원본 이메일의 복사본만 배치하며 이메일이 전달되는 것을 막지 못했습니다.이러한 콘텐츠 필터의 목적은 인바운드와 아웃바운드로 이동하는 이메일 유형에 대한 정보를 수집할 수 있도록 하기 위한 것입니다.

Content Filters(콘텐츠 필터) 보고서를 실행하고 격리에 저장된 이메일 사본을 검토한 후 "Duplicate message(메시지 복제)" 확인란 옵션의 선택을 취소하여 복사/복제 대신 원본 이메일을 격리에 넣는 것이 바람직합니다.