Guida alle best practice per i filtri contenuti in arrivo e in uscita

Sommario

Introduzione

I filtri contenuti consentono di esaminare i dettagli intricati di un messaggio e-mail e di eseguire azioni (o nessuna azione) sul messaggio. Dopo aver creato il filtro contenuto in ingresso o in uscita, applicarlo a un criterio di posta in arrivo o in uscita. Quando una e-mail corrisponde al filtro contenuti, il report "Content Filters" su Cisco Email Security Appliance (ESA) e Security Management Appliance (SMA) mostra tutte le e-mail che corrispondono a un filtro contenuti. Pertanto, anche se non viene intrapresa alcuna azione, è un ottimo modo per ottenere informazioni preziose sul tipo di e-mail che entrano e escono dall'organizzazione, consentendo di "modellare" il flusso di e-mail.

Poiché esistono molte "condizioni" e "azioni" diverse per i filtri contenuti, questo documento vi guiderà attraverso alcuni filtri contenuti in arrivo e in uscita molto comuni e consigliati.

Panoramica delle fasi

Passaggio 1: Importare i dizionari necessari

In questo documento vengono illustrati i passaggi necessari per l'implementazione di alcuni filtri per i contenuti in arrivo e in uscita basati su procedure ottimali. I filtri dei contenuti che creeremo faranno riferimento ad alcuni dizionari, quindi dovremo prima importarli. L'ESA viene fornita con i dizionari ed è sufficiente importarli nella configurazione per farvi riferimento nei filtri dei contenuti che creeremo.

Passaggio 2: Creare quarantene centralizzate

Per la maggior parte dei filtri contenuti, creeremo, imposteremo l'"azione" per mettere in quarantena l'e-mail (o una copia dell'e-mail) in una specifica (nuova) quarantena personalizzata, e quindi, dobbiamo prima creare quelle quarantene sull'SMA, in quanto questo documento presuppone che siano state abilitate le quarantene centralizzate PVO (Policy, Virus, and Outbreak) tra ESA e SMA.

Passaggio 3: Creazione di filtri dei contenuti in arrivo e in uscita e applicazione ai criteri

Una volta importati i dizionari e create le quarantene, verranno creati i filtri contenuti in arrivo e applicati ai criteri posta in arrivo, quindi verranno creati i filtri contenuti in uscita e applicati ai criteri posta in uscita.

PASSAGGIO 1: IMPORTAZIONE DEI DIZIONARI NECESSARI

Importazione dei dizionari a cui faremo riferimento nei nostri filtri contenuti:

- Sull'appliance ESA, selezionare **"Mail Policies > Dictionaries" (Policy di posta > Dizionari).**
- Fare clic sul pulsante "**Importa dizionario**" sul lato destro della pagina.

Profanità:

- Selezionare "**Importa dalla directory di configurazione dell'accessorio IronPort**".
- Selezionare "**profanity.txt**" e fare clic su "**Avanti**".
- Nome: **Profanity**
- Fare clic su "**Parole intere**" (MOLTO IMPORTANTE)
- Modificare i termini (aggiungere nuovi termini o rimuovere termini non desiderati)
- Fare clic su "**Submit" (Invia)**

Contenuto sessuale:

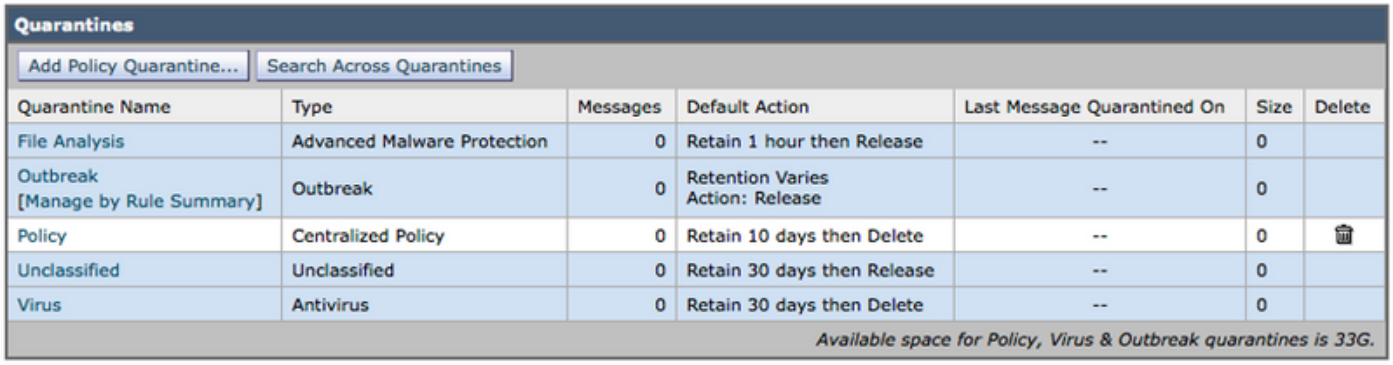
- Selezionare "**Importa dalla directory di configurazione dell'accessorio IronPort**".
- Selezionare "**sex_content.txt**" e fare clic su "**Avanti**".
- Nome: **SexualContent**
- Fare clic su "**Parole intere**" (MOLTO IMPORTANTE)
- Modificare i termini (aggiungere nuovi termini o rimuovere termini non desiderati)
- Fare clic su "**Submit" (Invia)**

Proprietario:

- Selezionare "**Importa dalla directory di configurazione dell'accessorio IronPort**".
- Selezionare "**proprietary_content.txt**" e fare clic su "**Avanti**".
- Nome: **Proprietario**
- Fare clic su "**Parole intere**" (MOLTO IMPORTANTE)
- Modificare i termini (aggiungere nuovi termini o rimuovere termini non desiderati)
- Fare clic su **"Submit" (Invia).**

PASSAGGIO 2: CREAZIONE DELLE QUARANTENE CENTRALIZZATE

- In SMA, selezionare **"Scheda E-mail > Quarantena messaggi > Quarantene PVO"**
- Ecco come dovrebbe apparire la tabella delle quarantene prima di iniziare. Tutte le quarantene sono predefinite.



- Fare clic sul pulsante **"Aggiungi quarantena criteri..."** pulsante
- Creare le quarantene seguenti.
- Alcuni verranno utilizzati dai filtri contenuti in arrivo, altri dai filtri contenuti in uscita. Le create allo stesso modo.

Quarantene PVO - utilizzate dai filtri contenuti in arrivo

URL dannoso in entrata:
Nome: URL dannoso in entrata
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Categoria URL in ingresso:
Nome: Categoria URL in ingresso
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Dati bancari in entrata:
Nome: Dati bancari in entrata
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

SSN in ingresso:
Nome: SSN in entrata
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

In ingresso non appropriato:
Nome: In ingresso non appropriato
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Errore hardware SPF:
Nome: Errore hardware SPF
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Errore software SPF:
Nome: Errore software SPF
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

SpoofMail:
Nome: SpoofMail
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Errore hardware DKIM:
Nome: Errore hardware DKIM
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Password protetta in ingresso:
Nome: Pwd Protetto In Entrata
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Quarantene PVO - utilizzate dai filtri contenuti in uscita

Dati bancari in uscita:
Nome: Dati bancari in uscita
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

SSN in uscita:
Nome: SSN in uscita
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

In uscita non appropriato:

URL dannoso in uscita:
Nome: URL dannoso in uscita
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Categoria URL in uscita:
Nome: Categoria URL in uscita
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Password protetta in uscita:

Nome: In uscita non appropriato
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

Nome: Pwd Protected Outbound
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

In uscita proprietario:
Nome: Outbound proprietario
Periodo di conservazione: 14 giorni
Azione predefinita: Elimina
Spazio disponibile: Attiva

- Ecco come dovrebbe apparire la tabella PVO dopo la creazione di tutte le quarantene PVO.

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.

PASSAGGIO 3: CREAZIONE DEI FILTRI DEI CONTENUTI IN ARRIVO

Dopo aver importato i dizionari e creato le quarantene di PVO, è possibile iniziare a creare i filtri contenuti in arrivo:

- Selezionare: **"Mail Policies > Incoming Content Filters" (Policy di posta > Filtri contenuti in arrivo)**
- Di seguito è riportata una tabella dei filtri contenuti in arrivo da creare. Ad esempio, sotto la tabella è riportato uno screenshot che illustra come creare il primo.

Crea questi filtri contenuti in arrivo

Nome: **Dati_banca**
Aggiungere Due Condizioni:
Corpo o allegato del messaggio:
Contiene Smart Identifier: Numero di routing ABA
Contiene Smart Identifier: Numero carta di credito
Aggiungi un'azione:

Quarantena:
Invia messaggio in quarantena: "Dati bancari in entrata (centralizzati)"
Messaggio duplicato: Attivato
(Notare che la regola di applicazione deve essere "Se una o più condizioni corrispondono")

Nome: **SSN**
Aggiungi una condizione:
Corpo o allegato del messaggio:
Contiene Smart Identifier: Numero SSN (Social Security Number)
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "SSN in entrata (centralizzato)"
Messaggio duplicato: Attivato
Nome: **Inappropriato**
Aggiungere Due Condizioni:
Corpo o allegato del messaggio:
Contiene il termine nel dizionario: Profanità
Contiene il termine nel dizionario: Contenuto_sessuale
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "In entrata non appropriato (centralizzato)"
Messaggio duplicato: Attivato
Nome: **Categoria_URL**
Aggiungi una condizione:
Categoria URL:
Seleziona categorie:
Adulti, Incontri, Prevenzione dei filtri, Freeware e Shareware, Giochi d'azzardo,
Giochi, Hacking, Lingerie e Costumi da bagno, Nudità non sessuale,
Domini in attesa, trasferimento file peer, pornografia
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "Categoria URL in entrata (centralizzata)"
Messaggio duplicato: Attivato
(Nota: Questo filtro contenuti richiede l'abilitazione di "Servizi di sicurezza"—> "Filtro URL")
Nome: **URL_Dannoso**
Aggiungi una condizione:
Reputazione URL:
Reputazione URL: Dannoso (da -10,0 a -6,0)
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "URL dannoso in entrata (centralizzato)"
Messaggio duplicato: Disabilitato (*** Metti in quarantena l'originale ****)
Nome: **Protetto da password**
Aggiungi una condizione:
Protezione allegati: Uno o più allegati sono protetti
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "Pwd protetto in entrata (centralizzato)"
Messaggio duplicato: Attivato
Nome: **Dimensione_10M**

Aggiungi una condizione:
  Dimensione messaggio:
    Maggiore o uguale a: 10 M
Aggiungi un'azione:
  Aggiungi tag messaggio:
    Immettere un termine: NOOP
(Nota: Ci deve essere un'azione in modo da qui "Tag" il messaggio per rappresentare nessuna operazione intrapresa. Il fatto che il filtro dei contenuti sia stato "Abbinato" consentirà di visualizzarlo nel report. Non è necessario eseguire alcuna operazione per visualizzarla in Reporting.)
Nome: **SPF_Hard_Fail**
Aggiungi una condizione:
  Verifica SPF: "is" Fail
Aggiungi un'azione:
  Quarantena:
    Invia messaggio in quarantena: "Errore hardware SPF (centralizzato)"
    Messaggio duplicato: Attivato
(Nota: "is Fail" è un errore di SPF hard e significa che il proprietario del dominio ti sta dicendo di eliminare tutte le email ricevute dai mittenti che non sono elencati nel loro record SPF. Inizialmente, è consigliabile utilizzare "Duplica messaggio" ed esaminare gli errori per una settimana o due prima di mettere in quarantena il messaggio originale (disattivando cioè i messaggi duplicati).
Nome: **SPF_Soft_Fail**
Aggiungi una condizione:
  Verifica SPF: "is" Softfail
Aggiungi un'azione:
  Quarantena:
    Invia messaggio in quarantena: "Errore software SPF (centralizzato)"
    Messaggio duplicato: Attivato
Nome: **DKIM_Hardfail_Copy**
Aggiungi una condizione:
  Autenticazione DKIM: "is" Hardfail
Aggiungere Due Azioni:
  Aggiungi/Modifica intestazione:
    Nome intestazione: Oggetto
    Fare clic su "Anteponi al valore dell'intestazione esistente" e immettere: [Copia - Non rilasciare]"
  Quarantena:
    Invia messaggio in quarantena: "DKIM Hard Fail (centralizzato)"
    Messaggio duplicato: Attivato
(Nota: Mettere in quarantena una copia del messaggio.)
Nome: **DKIM_Hardfail_Original**
Aggiungi una condizione:
  Autenticazione DKIM: "is" Hardfail
Aggiungi un'azione:
  Quarantena:
    Invia messaggio in quarantena: "DKIM Hard Fail (centralizzato)"
    Messaggio duplicato: Disattivato
(Nota: Verrà creata un'altra riga delle Regole sulla posta in arrivo per i domini PayPal ed eBay e verrà utilizzato questo filtro contenuti per i domini che devono superare la verifica DKIM.)
Nome: **Spoof_SPF_Failures**
Aggiungere una condizione, ma per entrambe le opzioni Softfail e Hardfail è selezionato:
  Verifica SPF: "is" Softfail e anche fare clic su "Fail"

(in modo da avere due caselle di controllo cliccato "Softfail" e "Fail"
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "SpoofMail (centralizzato)"
Messaggio duplicato: Attiva
(Nota: Utilizzeremo questo filtro contenuti per intervenire sulle e-mail in arrivo che fingono di inviare dal tuo dominio: lo spoofing. Iniziare con l'azione impostata per mettere in quarantena una copia e dopo un paio di settimane di revisione della quarantena SpoofMail, è possibile modificare il record DNS TXT SPF per aggiungere tutti i mittenti legittimi e a un certo punto, è possibile modificare questo filtro contenuti per mettere in quarantena l'originale disabilitando la casella di controllo del messaggio duplicato.)

Ad esempio, questo è l'aspetto che dovrebbe avere il filtro contenuto Bank_Data prima dell'invio.

Content Filter Settings

Name:	Bank_Data
RL Filtering — Currently Used by Policies:	Default Policy
Description:	
Order:	1 (of 7)

Conditions

Add Condition... | Apply rule: If one or more conditions match

Order	Condition	Rule	Delete
1	Message Body or Attachment	body-contains("*aba", 1)	
2	Message Body or Attachment	body-contains("*credit", 1)	

Actions

Add Action...

Order	Action	Rule	Delete
1	Quarantine	duplicate-quarantine("Bank Data Inbound")	

Dopo aver creato tutti i filtri contenuti in arrivo, la tabella dovrebbe avere il seguente aspetto:

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URLMalicious	Not in use		
2	URLCategory	Not in use		
3	SPFHardFail	Not in use		
4	Bank_Data	Not in use		
5	SSN	Not in use		
6	Inappropriate	Not in use		
7	URL_Category	Not in use		
8	URL_Malicious	Not in use		
9	Password_Protected	Not in use		
10	Size_10M	Not in use		
11	SPF_Hard_Fail	Not in use		
12	SPF_Soft_Fail	Not in use		
13	DKIM_Hardfail_Copy	Not in use		
14	DKIM_Hardfail_Original	Not in use		
15	Spoof_SPF_Failures	Not in use		

Edit Filter Order...

Poiché la funzione "Criteri" è selezionata (verrà visualizzato l'ipertesto Criteri nella parte superiore centrale), nella colonna centrale sono riportati i Criteri posta in arrivo a cui è stato applicato il filtro contenuti. Poiché non sono stati applicati ad alcun criterio Posta in arrivo, viene visualizzato il messaggio "Non in uso".

Applicazione dei filtri contenuti in arrivo ai criteri di posta in arrivo

- Accedere a: **"Mail Policies > Incoming Mail Policies" (Policy di posta in arrivo)**
- Fare clic sul testo **"Disabilitato"** nella cella Content Filters per **"Default Policy"**.
- Il pulsante del menu a discesa è impostato su **"Disabilita filtri contenuti"**.
- Fare clic sul pulsante e impostare su **"Abilita filtri contenuti"** per visualizzare immediatamente tutti i filtri contenuti in arrivo creati.
- Abilitare tutti i filtri tranne DKIM_Hardfail_Original e Spoof_SPF_Failures.
- **"Invia"** e "**Impegna"**.

Verifica DKIM per eBay e protezione tramite email contraffatte per il tuo dominio

Questi due argomenti riguardano i filtri contenuti che utilizzano la verifica DKIM e la verifica SPF. Per questo motivo, dobbiamo prima verificare che sia DKIM che SPF Verification siano abilitate.

1. Abilita verifica DKIM e SPF nei criteri di flusso della posta

- Accedere a: **"Criteri di posta > Criteri flusso di posta"**
- Abilitare la verifica DKIM e SPF in tutti i criteri di flusso della posta con "Comportamento connessione" impostato su "Accetto".
- Fare clic sull'ipertesto inferiore "Default Policy Parameters" e impostare **"DKIM Verification"** su **"On"** e **"SFP/SIDF Verification"** su **"On"**.
- Fare clic su **"Submit"** e **"Commit"**.
- Verrà visualizzata la tabella Criteri flusso di posta. Esaminare la colonna denominata **"Behavior"** e modificare qualsiasi criterio di flusso della posta con il comportamento impostato su **"Relay"**
- Disattiva **"Disattiva"** sia la verifica DKIM che SPF per i criteri di flusso della posta.
- Fare clic su **"Submit"** e **"Commit"**.

Non vogliamo che l'ESA esegua la verifica DKIM o SPF per i messaggi e-mail ricevuti nell'ESA dall'intestazione del server di posta Exchange in uscita. Nella maggior parte delle configurazioni, il criterio del flusso di posta "INOLTRATO" è l'unica riga con il comportamento di Inoltro.

2. Crea nuove Regole sul flusso della posta in arrivo per eBay e Paypal

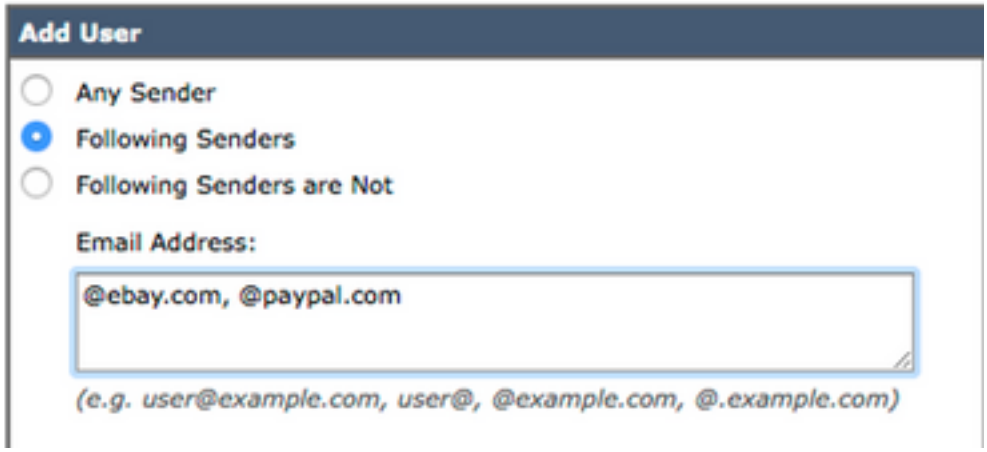
Le email in entrata ricevute da eBay e Paypal devono sempre superare la verifica DKIM. Verrà pertanto creato un altro criterio Posta in arrivo per utilizzare il filtro dei contenuti in arrivo DKIM_Hardfail_Original per i messaggi di posta elettronica provenienti da tali domini.

- Accedere a: **"Mail Policies > Incoming Mail Policies" (Policy di posta in arrivo)**
- Fare clic sul pulsante **"Aggiungi criterio"**.
- Immettere il nome: **"DKIM Hardfail Original"**
- Fare clic sul pulsante **"Aggiungi utente..."** pulsante.

Il pannello di configurazione successivo consente di definire i messaggi che soddisferanno il nuovo criterio Posta in arrivo. Si desidera solo definire i criteri per il mittente (la parte sinistra del

pannello di configurazione).

- Clic **"Mittenti successivi"** e nella tabella Indirizzi e-mail immettere **"@ebay.com, @paypal.com"**



- Fare clic sul pulsante **"OK"** pulsante in basso.
- Fare clic su **"Invia"**.

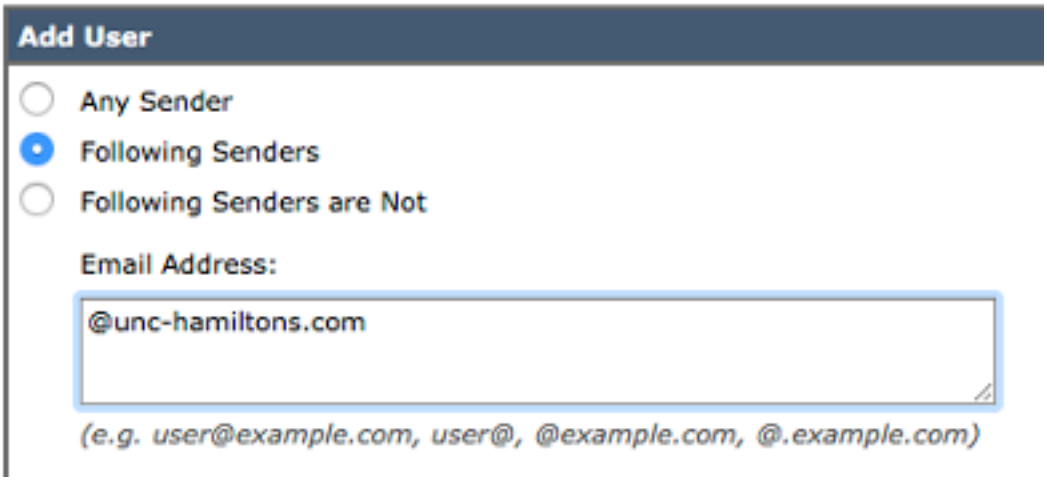
3. Crea un nuovo criterio flusso di posta in arrivo per il tuo dominio (protezione da spoof)

I passaggi in questa sezione consentono di eseguire azioni sui messaggi e-mail in arrivo con un indirizzo e-mail From del proprio dominio che non hanno superato la verifica SPF. Naturalmente, questo dipende dal fatto che avete già pubblicato il vostro record di testo SPF in DNS. Ignorare questi passaggi se non è stato creato/pubblicato un record di risorse testo SPF per il dominio.

- Accedere a: **"Mail Policies > Incoming Mail Policies" (Policy di posta in arrivo)**
- Fare clic sul pulsante **"Aggiungi criterio"**.
- Immettere il nome: **"Spoof_Protection"**
- Fare clic sul pulsante **"Aggiungi utente..."** pulsante.

Il pannello di configurazione successivo consente di definire i messaggi che corrisponderanno alla nuova riga Criteri posta in arrivo. Si desidera solo definire i criteri per il Mittente (che è la parte sinistra del pannello di configurazione).

- Fare clic sul pulsante **"Mittenti successivi"** e quindi immettere il dominio nella casella di testo **"Indirizzo e-mail:"**. Per me, il mio dominio è **"@unc-hamiltons.com"**



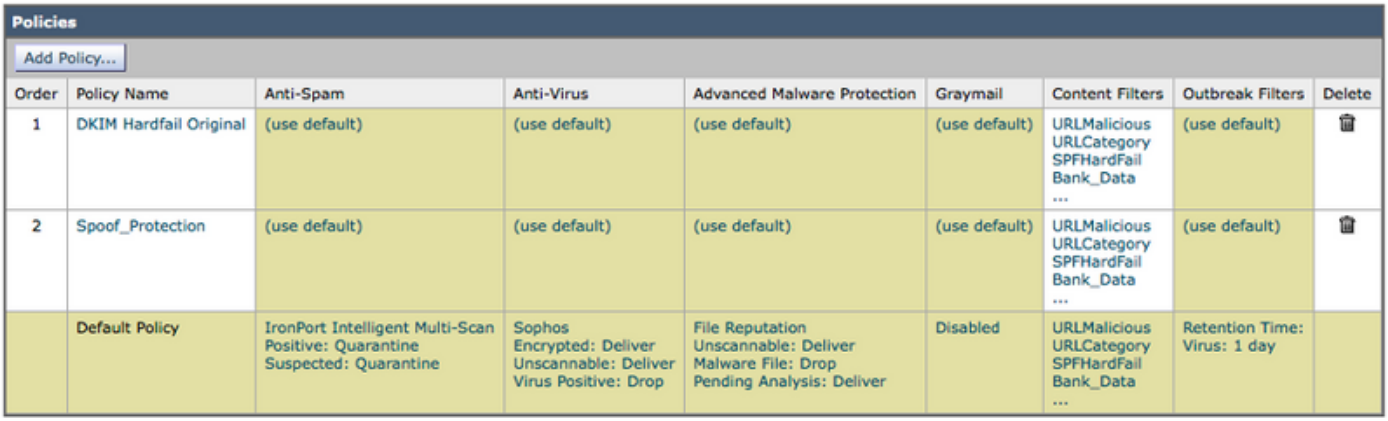
- Fare clic su **"Invia"**.

Viene visualizzata di nuovo la tabella Criteri posta in arrivo, ma al di sopra del criterio predefinito è

presente una seconda nuova riga Criteri posta.

- Fare clic sull'ipertesto **(predefinito)** nella cella Filtri contenuti per la nuova riga.
- Invertire il menu a discesa su **"Enable Content Filters (Customized Settings)"**.
- Controllare inoltre che sia **"DKIM_Hardfail_Copy"** che **"DKIM_Hardfail_Original"** non siano selezionate.
- Fare clic su **"Invia"** e su **"Conferma modifiche"**.

La tabella Criteri posta in arrivo dovrebbe avere il seguente aspetto:



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	

PASSAGGIO 4: CREAZIONE DEI FILTRI DEL CONTENUTO IN USCITA

- Passare a: **"Policy di posta > Filtri contenuti in uscita"**
- Di seguito è riportata una tabella dei filtri contenuti in uscita da creare.

Crea questi filtri contenuti in uscita

Nome: **Dati_banca**
Aggiungere Due Condizioni:
  Corpo o allegato del messaggio:
    Contiene Smart Identifier: Numero di routing ABA
    Contiene Smart Identifier: Numero carta di credito
Aggiungi un'azione:
  Quarantena:
    Invia messaggio in quarantena: "Dati bancari in uscita (centralizzati)"
    Messaggio duplicato: Attivato
(Notare che la regola di applicazione deve essere "Se una o più condizioni corrispondono")
Nome: **SSN**
Aggiungi una condizione:
  Corpo o allegato del messaggio:
    Contiene Smart Identifier: Numero SSN (Social Security Number)
Aggiungi un'azione:
  Quarantena:
    Invia messaggio in quarantena: "SSN in uscita (centralizzato)"
    Messaggio duplicato: Attivato
Nome: **Inappropriato**
Aggiungere Due Condizioni:
  Corpo o allegato del messaggio:
    Contiene il termine nel dizionario: Profanità
    Contiene il termine nel dizionario: Contenuto_sessuale
Aggiungi un'azione:
  Quarantena:
    Invia messaggio in quarantena: "In uscita non appropriato (centralizzato)"

Messaggio duplicato: Attivato
Nome: **Categoria_URL**
Aggiungi una condizione:
Categoria URL:
Seleziona categorie:
Adulti, Incontri, Prevenzione dei filtri, Freeware e Shareware, Giochi d'azzardo, Giochi, Hacking, Lingerie e Costumi da bagno, Nudità non sessuale, Domini in attesa, trasferimento file peer, pornografia
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "Categoria URL in uscita (centralizzata)"
Messaggio duplicato: Attivato
Nome: **URL_Dannoso**
Aggiungi una condizione:
Reputazione URL:
Reputazione URL: Dannoso (da -10,0 a -6,0)
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "URL dannoso in uscita (centralizzato)"
Messaggio duplicato: Disabilitato (*** Metti in quarantena l'originale ****)
Nome: **Protetto da password**
Aggiungi una condizione:
Protezione allegati: Uno o più allegati sono protetti
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "Pwd Protected Outbound (centralizzato)"
Messaggio duplicato: Attivato
Nome: **Dimensione_10M**
Aggiungi una condizione:
Dimensione messaggio:
Maggiore o uguale a: 10 M
Aggiungi un'azione:
Aggiungi tag messaggio:
Immettere un termine: NOOP
(Nota: Ci deve essere un'azione in modo da qui "Tag" il messaggio per rappresentare nessuna operazione intrapresa. Il fatto che il filtro dei contenuti sia stato "Abbinato" consentirà di visualizzarlo nel report. Non è necessario eseguire alcuna operazione per visualizzarla in Reporting.)
Nome: **Proprietario**
Aggiungi una condizione:
Corpo o allegato del messaggio:
Contiene il termine nel dizionario: Proprietario
Aggiungi un'azione:
Quarantena:
Invia messaggio in quarantena: "Proprietario (centralizzato)"
Messaggio duplicato: Attivato

Poiché la funzione "Criteri" è selezionata (verrà visualizzato l'ipertesto Criteri nella parte superiore centrale), la colonna centrale mostra i Criteri di posta in uscita a cui è stato applicato il filtro contenuti. Poiché non sono stati applicati ad alcun criterio di posta in uscita, viene visualizzato il messaggio "Non in uso".

- Accedere a: **"Mail Policies > Outgoing Mail Policies" (Policy di posta in uscita)**

- Fare clic sul testo **"Disabilitato"** nella cella Content Filters per il criterio predefinito.
- Il pulsante del menu a discesa è impostato su "**Disabilita filtri contenuti**".
- Fare clic sul pulsante e impostare su **"Abilita filtri contenuti"** per visualizzare immediatamente tutti i filtri contenuti in uscita creati.
- **"Abilita"** tutti i filtri.
- **"Invia"** e **"Esegui"**.

Riepilogo

Sono state implementate le procedure ottimali iniziali per i filtri dei contenuti in arrivo e in uscita. La maggior parte dei filtri contenuti (non tutti) ha utilizzato l'azione di quarantena e ha scelto di selezionare (abilitare) l'opzione "Duplica messaggio", che si limita a inserire una copia dell'e-mail originale e non impedisce il recapito dell'e-mail. Lo scopo di questi filtri dei contenuti è quello di consentire la raccolta di informazioni sui tipi di e-mail in entrata e in uscita verso la società.

Detto questo, dopo aver eseguito il report Content Filters e aver controllato le copie e-mail salvate nelle quarantene, può essere prudente deselezionare l'opzione "Duplica messaggio" e quindi iniziare a mettere l'e-mail originale in quarantena invece di una copia/duplicato.