Best Practices-Leitfaden für Filter für eingehende und ausgehende Inhalte

Inhalt

Einführung

Mit Content-Filtern können Sie detaillierte Details einer E-Mail überprüfen und Aktionen (oder keine Aktion) für die E-Mail ausführen. Sobald der Filter für eingehende oder ausgehende Inhalte erstellt wurde, wenden Sie ihn auf eine Richtlinie für eingehende oder ausgehende E-Mails an. Wenn eine E-Mail mit dem Content-Filter übereinstimmt, können Sie im Bericht "Content-Filter" der Cisco E-Mail Security Appliance (ESA) und der Security Management Appliance (SMA) alle E-Mails anzeigen, die einem Content-Filter entsprechen. Auch wenn keine Maßnahmen ergriffen werden, ist dies eine hervorragende Möglichkeit, wertvolle Informationen über die Art von E-Mails zu erhalten, die in Ihr Unternehmen eingehen und aus diesem ausgehen. So können Sie Ihren E-Mail-Fluss "Muster" eingeben.

Da es viele verschiedene Inhaltsfilter-"Bedingungen" und "Aktionen" gibt, wird dieses Dokument Sie durch einige sehr häufig verwendete und empfohlene Filter für eingehende und ausgehende Inhalte führen.

Überblick über die Schritte

Schritt 1: Importieren der benötigten Wörterbücher

Dieses Dokument enthält die erforderlichen Schritte zur Implementierung einiger Filter für eingehende und ausgehende Inhalte mit Best Practices. Die von uns erstellten Inhaltsfilter beziehen sich auf einige Wörterbücher. Daher müssen wir diese Wörterbücher zuerst importieren. Die ESA wird mit den Wörterbüchern ausgeliefert. Sie müssen diese lediglich in die Konfiguration importieren, um sie in den von uns erstellten Inhaltsfiltern zu finden.

Schritt 2: Erstellen einer zentralen Quarantäne

Für die meisten Content-Filter legen wir die Aktion auf Quarantäne der E-Mail (oder eine Kopie der E-Mail) in eine angegebene benutzerdefinierte (neue) Quarantäne fest. Daher müssen diese Quarantänen zuerst im SMA erstellt werden, da in diesem Dokument davon ausgegangen wird, dass Sie die zentrale PVO-Quarantäne (Policy, Virus, Outbreak) zwischen der ESA und SMA

aktiviert haben.

Schritt 3: Erstellen Sie die Filter für eingehende und ausgehende Inhalte, und wenden Sie diese auf Richtlinien an.

Nachdem die Wörterbücher importiert und die Quarantäne erstellt wurden, erstellen wir die Filter für eingehende Inhalte und wenden sie auf die Richtlinien für eingehende E-Mails an. Anschließend erstellen wir die Filter für ausgehende Inhalte und wenden sie auf die Richtlinien für ausgehende E-Mails an.

SCHRITT 1: IMPORTIEREN DER BENÖTIGTEN WÖRTERBÜCHER

Importieren der Wörterbücher, auf die wir in unseren Inhaltsfiltern verweisen werden:

- Navigieren Sie auf der ESA-Appliance zu **"Mail Policies > Dictionaries".**
- Klicken Sie auf der rechten Seite auf die Schaltfläche **Dictionary importieren**.

Rentabilität:

- Wählen Sie "**Importieren aus dem Konfigurationsverzeichnis der IronPort-Appliance**" aus.
- Wählen Sie "**profanity.txt**" aus, und klicken Sie auf "**Weiter**".
- Name: **Profanity**
- Klicken Sie auf "**Vollständige Wörter zuordnen**" (SEHR WICHTIG).
- Bearbeiten Sie die Begriffe (Hinzufügen neuer Begriffe oder Entfernen unerwünschter Begriffe).
- Klicken Sie auf "**Senden".**

Sexuelle Inhalte:

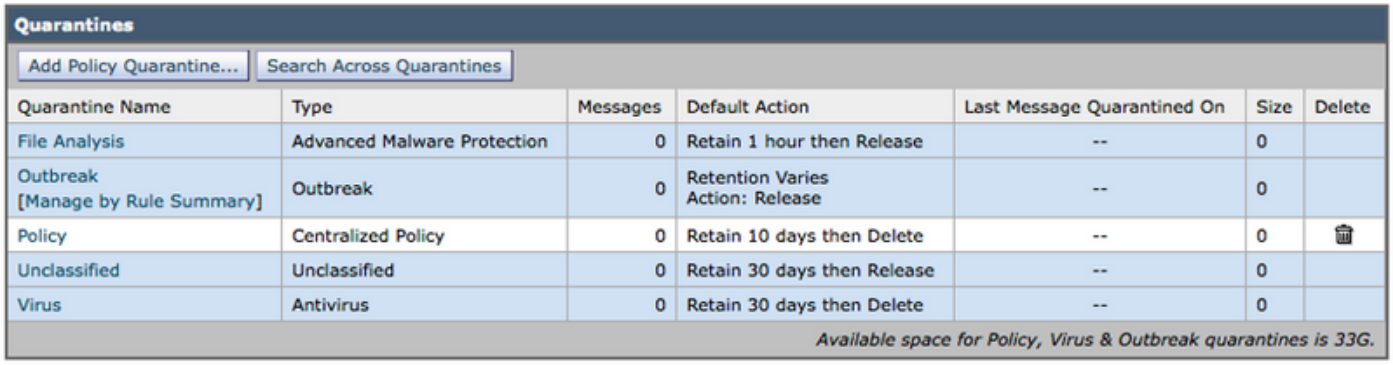
- Wählen Sie "**Importieren aus dem Konfigurationsverzeichnis der IronPort-Appliance**" aus.
- Wählen Sie "**sex_content.txt**" und klicken Sie auf "**Weiter**".
- Name: **SexualContent**
- Klicken Sie auf "**Vollständige Wörter zuordnen**" (SEHR WICHTIG).
- Bearbeiten Sie die Begriffe (Hinzufügen neuer Begriffe oder Entfernen unerwünschter Begriffe).
- Klicken Sie auf "**Senden".**

Urheberrechtlich geschützt:

- Wählen Sie "**Importieren aus dem Konfigurationsverzeichnis der IronPort-Appliance**" aus.
- Wählen Sie "**proprietär_content.txt**" und klicken Sie auf "**Weiter**".
- Name: **proprietär**
- Klicken Sie auf "**Vollständige Wörter zuordnen**" (SEHR WICHTIG).
- Bearbeiten Sie die Begriffe (Hinzufügen neuer Begriffe oder Entfernen unerwünschter Begriffe).
- Klicken Sie auf **"Senden".**

SCHRITT 2: ERSTELLEN DER ZENTRALISIERTEN QUARANTINEN

- Navigieren Sie im SMA zu **"Email Tab > Message Quarantine > PVO Quarantines".**
- So sollte die Quarantänetabelle aussehen, bevor wir beginnen. Alle Quarantänen sind standardmäßig aktiviert.



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.

- Klicken Sie auf **"Policy Quarantine hinzufügen.."** Schaltfläche
- Erstellen Sie die folgenden Quarantänebereiche.
- Einige werden von den Filtern für eingehende Inhalte verwendet, andere von den Filtern für ausgehende Inhalte. Sie erstellen sie auf die gleiche Weise.

PVO-Quarantänen - Verwendung durch Filter für eingehende Inhalte

URL: bösartiger eingehender Datenverkehr:
Name: Bösartige eingehende URLs
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Eingehende URL-Kategorie:
Name: Eingehende URL-Kategorie
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Bankdaten für eingehenden Datenverkehr:
Name: Bankdaten eingehend
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Eingehender SSN-Datenverkehr:
Name: Eingehendes SSN
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Unangemessener eingehender Datenverkehr:
Name: Unangemessener eingehender Datenverkehr
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

SPF-Hard Fail:
Name: SPF-Hard Fail
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

SPF-Soft-Fail:
Name: SPF-Soft-Failover
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

SpoofMail:
Name: SpoofMail
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

DKIM-Hard Failover:
Name: DKIM-Hard Failover
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Eingehender Kennwortschutz:
Name: Eingehender PWD-Schutz
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

PVO-Quarantänen - Verwendung durch Filter für ausgehende Inhalte

Ausgehende Bankdaten:
Name: Ausgehende Bankdaten
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Ausgehendes SSN:
Name: Ausgehendes SSN

URL-schädlich für ausgehenden Datenverkehr:
Name: URL-schädlich für ausgehenden Datenverkehr
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

URL-Kategorie ausgehend:
Name: URL-Kategorie ausgehend

Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Unangemessener ausgehender Datenverkehr:
Name: Unangemessener ausgehender Datenverkehr
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Proprietäres Outbound:
Name: Proprietäres Outbound
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

Kennwortschutz für ausgehenden Datenverkehr:
Name: Von PWD geschützter ausgehender Datenverkehr
Aufbewahrungszeitraum: 14 Tage
Standardaktion: Löschen
Freier Speicherplatz: Aktivieren

- Hier sehen Sie, wie Ihre PVO-Tabelle darauf achten sollte, alle PVO-Quarantänen zu erstellen.

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.

SCHRITT 3: ERSTELLEN DER EINGEHENDEN INHALTSFILTER

Nachdem die Wörterbücher importiert und die PVO-Quarantäne erstellt wurden, können Sie jetzt mit der Erstellung der Filter für eingehende Inhalte beginnen:

- Navigieren Sie zu **"Mail-Policys > Filter für eingehende Inhalte".**
- Die folgende Tabelle enthält die Filter für eingehende Inhalte, die Sie erstellen sollten. In der Tabelle unten sehen Sie beispielsweise einen Screenshot, in dem veranschaulicht wird, wie die erste erstellt wird.

Erstellen Sie diese Filter für eingehende Inhalte.

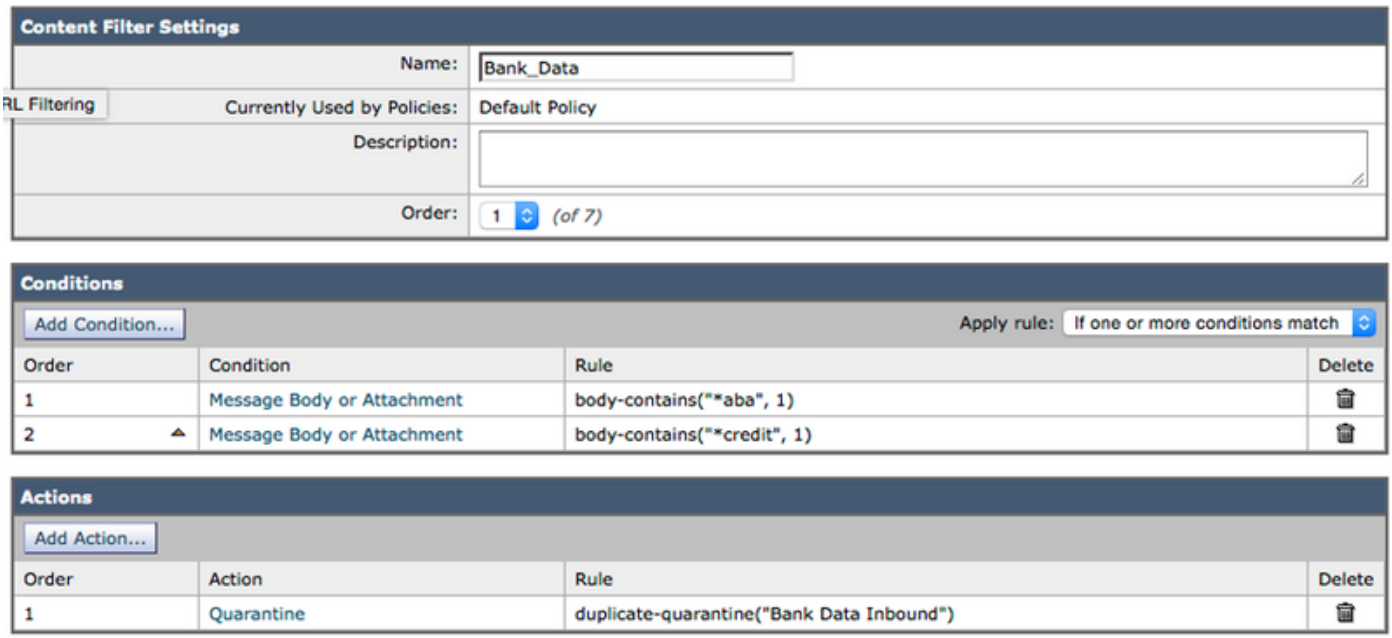
Name: **Bank_Daten**
Fügen Sie zwei Bedingungen hinzu:
  Nachrichtentext oder Anlage:
    Enthält Smart Identifier: ABA-Weiterleitungsnummer
    Enthält Smart Identifier: Kreditkartennummer
Eine Aktion hinzufügen:
  Quarantäne:
    Nachricht an Quarantäne senden: "Bank Data Inbound (zentralisiert)"
    Doppelte Nachricht: Aktiviert
(Beachten Sie, dass die Regel "Wenn eine oder mehrere Bedingungen übereinstimmen" lautet.)
Name: **SSN**
Eine Bedingung hinzufügen:
  Nachrichtentext oder Anlage:
    Enthält Smart Identifier: Sozialversicherungsnummer (SSN)
Eine Aktion hinzufügen:
  Quarantäne:
    Nachricht an Quarantäne senden: "SSN Inbound (zentralisiert)"
    Doppelte Nachricht: Aktiviert
Name: **Unpassend**
Fügen Sie zwei Bedingungen hinzu:
  Nachrichtentext oder Anlage:
    Enthält einen Begriff im Wörterbuch: Profanität
    Enthält einen Begriff im Wörterbuch: Sexuelle Inhalte
Eine Aktion hinzufügen:
  Quarantäne:
    Nachricht an Quarantäne senden: "Unangemessener eingehender (zentralisierter) Datenverkehr"
    Doppelte Nachricht: Aktiviert
Name: **URL_Kategorie**
Eine Bedingung hinzufügen:
  URL-Kategorie:
    Kategorien auswählen:
      Erwachsene, Daten, Filtervermeidung, Freeware und Shareware, Glücksspiel, Spiele, Hacking, Fingerie und Swimsuits, nicht sexuelle Nacktheit, Parkplätze für Domänen, Übertragung von Peer-Dateien, Pornografie
Eine Aktion hinzufügen:
  Quarantäne:
    Nachricht an Quarantäne senden: "URL-Kategorie Eingehend (zentralisiert)"
    Doppelte Nachricht: Aktiviert
(Hinweis: Dieser Content-Filter erfordert die Aktivierung von "Security Services"—> "URL-Filterung")
Name: **URL_schädlich**
Eine Bedingung hinzufügen:
  URL-Reputation:
    URL-Reputation: Schädlich (-10,0 bis -6,0)
Eine Aktion hinzufügen:
  Quarantäne:
    Nachricht an Quarantäne senden: "URL Malicious Inbound (zentralisiert)"
    Doppelte Nachricht: Deaktiviert (**** Quarantäne für das Original ****)
Name: **Kennwort_geschützt**
Eine Bedingung hinzufügen:

Schutz von Anhängen: Mindestens eine Anlage ist geschützt
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "Pwd Protected Inbound (zentralisiert)"
Doppelte Nachricht: Aktiviert
Name: **Größe_10 Mio.**
Eine Bedingung hinzufügen:
Nachrichtengröße:
größer oder gleich: 10 Mio.
Eine Aktion hinzufügen:
Nachrichtentag hinzufügen:
Begriff eingeben: NOOP
(Hinweis: Es muss eine Aktion geben, daher stellen wir hier die Nachricht "Tag" (Tagging) dar, dass kein Vorgang durchgeführt wurde. Die Tatsache, dass der Content-Filter "Matched" (Übereinstimmend) ist, ermöglicht es ihm, sich im Reporting anzuzeigen. Es müssen keine "Maßnahmen" ergriffen werden, um in Reporting angezeigt zu werden.)
Name: **SPF_Hard_Fail**
Eine Bedingung hinzufügen:
SPF-Verifizierung: Fehlschlag
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "SPF Hard Fail (zentralisiert)"
Doppelte Nachricht: Aktiviert
(Hinweis: "is Fail" ist ein Hard SPF-Fehler und das bedeutet, dass der Besitzer der Domäne Ihnen mitteilt, alle E-Mails von Absendern zu löschen, die nicht in ihrem SPF-Datensatz aufgeführt sind. Es empfiehlt sich zunächst, "Duplicate Message" zu verwenden und die Fehler für ein oder zwei Wochen zu überprüfen, bevor das Original unter Quarantäne gestellt wird (d. h. doppelte Nachrichten zu deaktivieren).
Name: **SPF_Soft_Fail**
Eine Bedingung hinzufügen:
SPF-Verifizierung: "is"-Softfail
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "SPF Soft Fail (zentralisiert)"
Doppelte Nachricht: Aktiviert
Name: **DKIM_Hardfail_Kopie**
Eine Bedingung hinzufügen:
DKIM-Authentifizierung: Hardware ist fehlerhaft
Zwei Aktionen hinzufügen:
Header hinzufügen/bearbeiten:
Header-Name: Betreff
Klicken Sie auf "Dem Wert des vorhandenen Headers voranstellen", und geben Sie Folgendes ein: [Kopieren - Nicht freigeben]"
Quarantäne:
Nachricht an Quarantäne senden: "DKIM Hard Fail (zentralisiert)"
Doppelte Nachricht: Aktiviert
(Hinweis: Eine Kopie der Nachricht zunächst in Quarantäne stellen.)
Name: **DKIM_Hardfail_Original**
Eine Bedingung hinzufügen:
DKIM-Authentifizierung: Hardware ist fehlerhaft
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "DKIM Hard Fail (zentralisiert)"

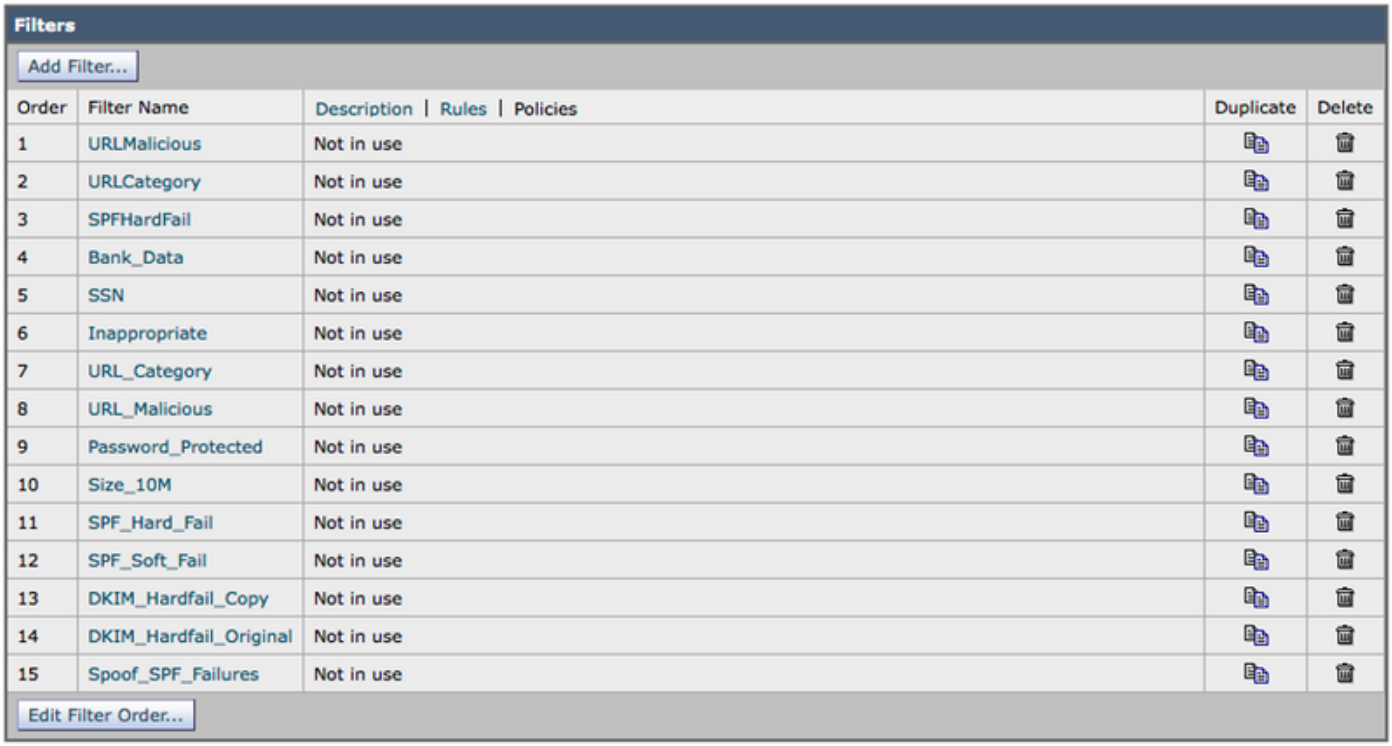
Doppelte Nachricht: Deaktiviert
(Hinweis: Wir erstellen eine weitere Reihe von Richtlinien für eingehende E-Mails für PayPal- und eBay-Domänen und verwenden diesen Content-Filter für Domänen, von denen wir wissen, dass sie die DKIM-Verifizierung bestehen sollten.)

Name: **Spoof_SPF_Failure**
Fügen Sie eine Bedingung hinzu, aber SOWOHL SOFTWARE- als auch Hardware-Failover-Prüfung ist aktiviert:
SPF-Verifizierung: "is" Softfail und auch "Fail" (Fehler) anklicken
(Sie haben also zwei Kontrollkästchen aktiviert, die auf "Softfail" (Softfail) und "Fail" (Fehler) geklickt haben.
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "SpoofMail (zentralisiert)"
Doppelte Nachricht: Aktivieren
(Hinweis: Wir werden diesen Content-Filter verwenden, um Maßnahmen für eingehende E-Mails zu ergreifen, die vorgeben, von Ihrer eigenen Domäne aus - Spoofing - zu senden. Beginnen Sie mit der Aktion, eine Kopie unter Quarantäne zu stellen. Nach einigen Wochen der Überprüfung der SpoofMail-Quarantäne können Sie Ihren SPF TXT DNS-Datensatz so ändern, dass alle legitimen Absender hinzugefügt werden. Sie können diesen Content-Filter irgendwann ändern, um das Original zu isolieren, indem Sie das Kontrollkästchen für die doppelte Nachricht deaktivieren.)

So sollte der Content-Filter Bank_Data beispielsweise aussehen, bevor Sie Daten senden.



Nachdem Sie alle Filter für eingehende Inhalte erstellt haben, sollte die Tabelle nun wie folgt aussehen:



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...

Da die Funktion "Policies" ausgewählt ist (der Hypertext Policies (Richtlinien) wird oben in der Mitte angezeigt), werden in der mittleren Spalte die Richtlinien für eingehende E-Mails angezeigt, auf die der Content-Filter angewendet wurde. Da wir sie nicht auf eine Richtlinie für eingehende E-Mails angewendet haben, wird die Meldung "Nicht verwendet" angezeigt.

Wenden Sie die Filter für eingehende Inhalte auf die Richtlinien für eingehende E-Mails an.

- Navigieren Sie zu: **"Mail-Policys > Mail-Policys für \"Eingehend\"**
- Klicken Sie für die **Standardrichtlinie** in der Zelle Inhaltsfilter auf den **"Disabled"**-Text.
- Die Pulldown-Menütaste ist auf **"Content-Filter deaktivieren"** eingestellt.
- Klicken Sie auf die Schaltfläche, und legen Sie **"Content-Filter aktivieren"** fest. Daraufhin werden Ihnen umgehend alle erstellten Filter für eingehende Inhalte angezeigt.
- Aktivieren Sie alle Filter außer DKIM_Hardfail_Original und Spoof_SPF_Failures.
- **"Senden"** und "**Bestätigen"**.

DKIM Verification for eBay & Paypal and Spoof Email Protection für Ihre Domäne

Diese beiden Themen betreffen Content-Filter, die die DKIM-Verifizierung und die SPF-Verifizierung verwenden. Daher müssen zunächst sowohl die DKIM- als auch die SPF-Verifizierung aktiviert werden.

1. Aktivieren der DKIM- und SPF-Verifizierung in Mail Flow-Richtlinien

- Navigieren Sie zu: **"Mail Policies > Mail Flow Policies" (Mail-Policys > Mail Flow-Policys)**
- Aktivieren Sie die DKIM- und SPF-Verifizierung in allen Mail Flow-Richtlinien, die "Connection Behavior" (Verbindungsverhalten) von "Accept" (Akzeptieren) aufweisen.
- Klicken Sie auf den unteren Hypertext **"Default Policy Parameters"** und setzen Sie **"DKIM Verification"** auf **"On"** und **"SFP/SIDF Verification"** auf **"On".**
- Klicken Sie auf **"Senden"** und **"Bestätigen"**.
- Sie sehen nun die Tabelle Mail Flow Policies (Mail-Ablaufrichtlinien). Betrachten Sie die

Spalte **"Behavior"** und bearbeiten Sie alle Mail Flow-Richtlinien, wobei das Verhalten auf **"Relay"** festgelegt ist.
- Deaktivieren Sie sowohl die DKIM- als auch die SPF-Verifizierung für diese Mail-Flow-Richtlinien.
- Klicken Sie auf **"Senden"** und **"Bestätigen"**.

Die ESA soll keine DKIM- oder SPF-Überprüfung für E-Mails durchführen, die von der Überschrift des Exchange-Mail-Servers ausgehend in die ESA empfangen wurden. In den meisten Konfigurationen ist die "RELAYED" Mail Flow Policy die einzige Zeile mit dem Behavior of Relay.

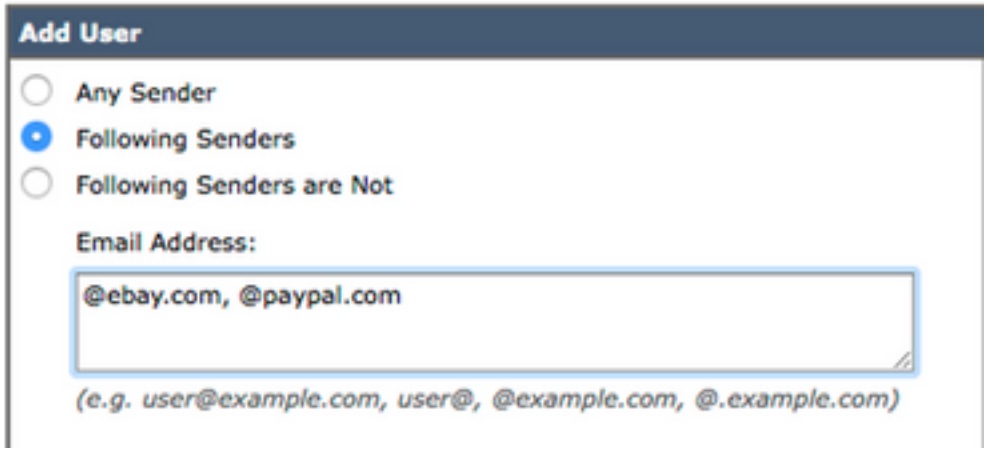
2. Erstellen einer neuen Richtlinie für den Fluss eingehender E-Mails für eBay und Paypal

Eingehende E-Mails, die von eBay und Paypal empfangen wurden, sollten immer die DKIM-Verifizierung bestehen. Wir erstellen daher eine weitere Richtlinie für eingehende E-Mails, um den Filter "DKIM_Hardfail_Original Incoming Content" für eine E-Mail aus diesen Domänen zu verwenden.

- Navigieren Sie zu: **"Mail-Policys > Mail-Policys für \"Eingehend\"**
- Klicken Sie auf die Schaltfläche **"Richtlinie hinzufügen"**.
- Geben Sie den Namen ein: **"DKIM Hardfail Original"**
- Klicken Sie auf **"Benutzer hinzufügen.."** -Taste.

Im nächsten Konfigurationsfenster können Sie festlegen, welche Nachrichten dieser neuen Richtlinie für eingehende E-Mails entsprechen. Wir möchten nur die Kriterien für den Absender definieren (der linke Teil des Konfigurationsbereichs).

- Klicken **"Absender folgen"** und geben Sie in der Tabelle "E-Mail-Adressen" **@ ein.ebay.com, @paypal.com"**



- Klicken Sie auf **OK** unten.
- Klicken Sie **"Senden"**.

3. Erstellen einer neuen Richtlinie für den eingehenden E-Mail-Fluss für Ihre Domäne (Spoof Protection)

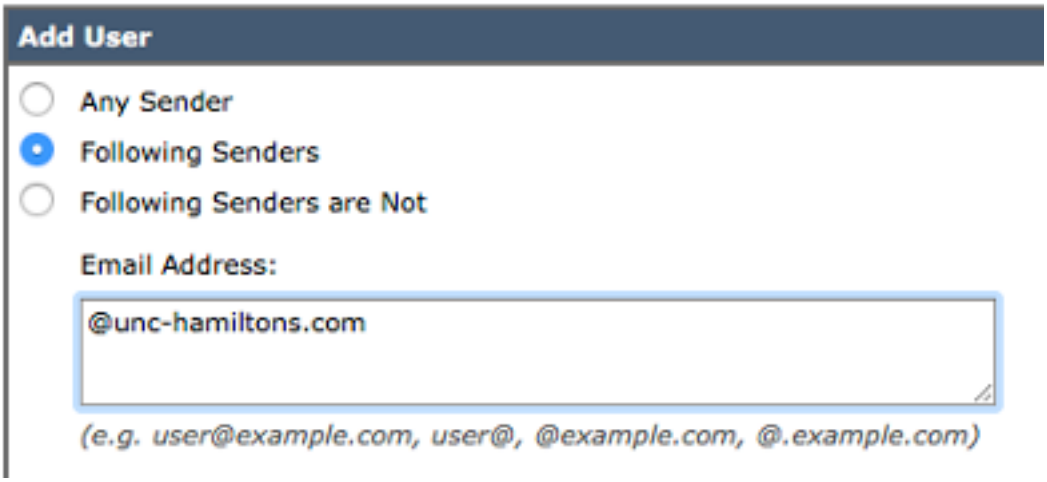
Mit den Schritten in diesem Abschnitt können Sie Maßnahmen für eingehende E-Mails ergreifen, die über eine Von-E-Mail-Adresse Ihrer eigenen Domäne verfügen und die nicht SPF-verifiziert werden können. Dies hängt natürlich davon ab, dass Sie Ihren SPF-Textdatensatz bereits im DNS veröffentlicht haben. Überspringen Sie diese Schritte, wenn Sie keinen SPF-Textressourcendatensatz für Ihre Domäne erstellt/veröffentlicht haben.

- Navigieren Sie zu: **"Mail-Policys > Mail-Policys für \"Eingehend\"**

- Klicken Sie auf die Schaltfläche **"Richtlinie hinzufügen"**.
- Geben Sie den Namen ein: **"Spoof_Protection"**
- Klicken Sie auf **"Benutzer hinzufügen.."** -Taste.

Im nächsten Konfigurationsfenster können Sie festlegen, welche Nachrichten dieser neuen Zeile für die Richtlinie für eingehende E-Mails entsprechen. Sie möchten nur die Kriterien für den Absender definieren (dies ist der linke Teil des Konfigurationsbereichs).

- Klicken Sie auf **"Absender folgen"** und geben Sie dann Ihre Domäne in das Textfeld **"E-Mail-Adresse:"** ein. Für mich ist meine Domäne **"@unc-hamiltons.com".**



- Klicken Sie **"Senden"**.

Sie erhalten erneut die Tabelle "Incoming Mail Policies" (Richtlinien für eingehende E-Mails), aber jetzt haben Sie eine zweite neue E-Mail-Policy-Zeile oberhalb der Standard-Policy.

- Klicken Sie in der Zelle Inhaltsfilter für die neue Zeile auf den **(standardmäßig verwendeten)** Hypertext.
- Wechseln Sie im Pulldown-Menü zu **"Inhaltsfilter aktivieren (benutzerdefinierte Einstellungen)"**.
- Prüfen Sie den **"Spoof_SPF_Failures"**, und stellen Sie sicher, dass sowohl **"DKIM_Hardfail_Copy"** als auch **"DKIM_Hardfail_Original"** deaktiviert sind.
- Klicken Sie auf **"Senden"** und **"Änderungen bestätigen"**.

Die Tabelle für eingehende Mail-Policys sollte nun wie folgt aussehen:

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	

SCHRITT 4: ERSTELLEN DER AUSGEHENDEN INHALTSFILTER

- Navigieren Sie zu **"Mail-Policys > Filter für ausgehende Inhalte".**

- Die folgende Tabelle enthält ausgehende Inhaltsfilter, die Sie erstellen sollten.

Erstellen Sie diese Filter für ausgehende Inhalte.

Name: **Bank_Daten**
Fügen Sie zwei Bedingungen hinzu:
Nachrichtentext oder Anlage:
Enthält Smart Identifier: ABA-Weiterleitungsnummer
Enthält Smart Identifier: Kreditkartennummer
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "Ausgehende Bankdaten (zentralisiert)"
Doppelte Nachricht: Aktiviert
(Beachten Sie, dass die Regel "Wenn eine oder mehrere Bedingungen übereinstimmen" lautet.)
Name: **SSN**
Eine Bedingung hinzufügen:
Nachrichtentext oder Anlage:
Enthält Smart Identifier: Sozialversicherungsnummer (SSN)
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "SSN Outbound (zentralisiert)"
Doppelte Nachricht: Aktiviert
Name: **Unpassend**
Fügen Sie zwei Bedingungen hinzu:
Nachrichtentext oder Anlage:
Enthält einen Begriff im Wörterbuch: Profanität
Enthält einen Begriff im Wörterbuch: Sexuelle Inhalte
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "Unangemessener ausgehender Datenverkehr (zentralisiert)"
Doppelte Nachricht: Aktiviert
Name: **URL_Kategorie**
Eine Bedingung hinzufügen:
URL-Kategorie:
Kategorien auswählen:
Erwachsene, Daten, Filtervermeidung, Freeware und Shareware, Glücksspiel, Spiele, Hacking, Fingerie und Swimsuits, nicht sexuelle Nacktheit, Parkplätze für Domänen, Übertragung von Peer-Dateien, Pornografie
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "URL-Kategorie Outbound (zentralisiert)"
Doppelte Nachricht: Aktiviert
Name: **URL_schädlich**
Eine Bedingung hinzufügen:
URL-Reputation:
URL-Reputation: Schädlich (-10,0 bis -6,0)
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "URL Malicious Outbound (zentralisiert)"
Doppelte Nachricht: Deaktiviert (**** Ursprüngliche Quarantäne ***)
Name: **Kennwort_geschützt**
Eine Bedingung hinzufügen:
Schutz von Anhängen: Mindestens eine Anlage ist geschützt

Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "Pwd Protected Outbound (zentralisiert)"
Doppelte Nachricht: Aktiviert
Name: **Größe_10 Mio.**
Eine Bedingung hinzufügen:
Nachrichtengröße:
größer oder gleich: 10 Mio.
Eine Aktion hinzufügen:
Nachrichtentag hinzufügen:
Begriff eingeben: NOOP
(Hinweis: Es muss eine Aktion geben, daher stellen wir hier die Nachricht "Tag" (Tagging) dar, dass kein Vorgang durchgeführt wurde. Die Tatsache, dass der Content-Filter "Matched" (Übereinstimmend) ist, ermöglicht es ihm, sich im Reporting anzuzeigen. Es müssen keine "Maßnahmen" ergriffen werden, um in Reporting angezeigt zu werden.)
Name: **Proprietär**
Eine Bedingung hinzufügen:
Nachrichtentext oder Anlage:
Enthält einen Begriff im Wörterbuch: Proprietär
Eine Aktion hinzufügen:
Quarantäne:
Nachricht an Quarantäne senden: "Proprietär (zentralisiert)"
Doppelte Nachricht: Aktiviert

Da die Funktion "Policies" (Richtlinien) ausgewählt ist (der Hypertext Policies (Richtlinien) wird oben in der Mitte angezeigt), werden in der mittleren Spalte die Richtlinien für ausgehende E-Mails angezeigt, auf die der Content-Filter angewendet wurde. Da wir sie nicht auf eine Richtlinie für ausgehende E-Mails angewendet haben, wird "Nicht verwendet" angezeigt.

- Navigieren Sie zu: **"Mail-Policys > Mail-Policys für \"Ausgehend\"**
- Klicken Sie für die Standardrichtlinie auf den **Text "Deaktiviert"** in der Zelle Inhaltsfilter.
- Die Pulldown-Menütaste ist auf "**Content-Filter deaktivieren**" eingestellt.
- Klicken Sie auf die Schaltfläche, und legen Sie **"Content-Filter aktivieren"** fest. Daraufhin werden Ihnen umgehend alle erstellten Filter für ausgehende Inhalte angezeigt.
- **"Aktivieren"** alle Filter.
- **"Senden"** und **"Bestätigen"**.

Zusammenfassung

Sie haben jetzt erste Best Practices für Filter für eingehende und ausgehende Inhalte implementiert. Die meisten (nicht alle) Content-Filter verwendeten die Quarantäneaktion und aktivierten die Option "Doppelte Nachricht" (Aktivieren). Diese Option platziert lediglich eine Kopie der ursprünglichen E-Mail und verhindert nicht, dass die E-Mail zugestellt wird. Mit diesen Content-Filtern können Sie Informationen zu den E-Mails sammeln, die ein- und ausgehende Nachrichten an Ihr Unternehmen senden.

Allerdings ist es nach der Ausführung des Content-Filters-Berichts und dem Durchsuchen der in der Quarantäne gespeicherten E-Mail-Kopien ratsam, die Option "Doppelte Nachricht" zu deaktivieren und damit anstelle einer Kopie/doppelten Kopie die ursprüngliche E-Mail in die Quarantäne zu stellen.