Guía de prácticas recomendadas para filtros de contenido entrante y saliente

Contenido

Introducción

Los filtros de contenido permiten inspeccionar los detalles complejos de un mensaje de correo electrónico y realizar acciones (o ninguna acción) en el mensaje de correo electrónico. Una vez creado el filtro de contenido entrante o saliente, se lo aplica a una política de correo entrante o saliente. Cuando cualquier correo electrónico coincida con el filtro de contenido, el informe "Filtros de contenido" del dispositivo de seguridad Cisco Email Security Appliance (ESA) y el dispositivo de gestión de seguridad (SMA) podrán mostrarle todos los correos electrónicos que coincidan con cualquier filtro de contenido. Por lo tanto, aunque no se realice ninguna acción, se trata de una forma excelente de obtener información valiosa sobre el tipo de mensajes de correo electrónico que entran y salen de la organización, lo que le permite "modelar" su flujo de correo electrónico.

Dado que hay muchas "Condiciones" y "Acciones" de filtros de contenido diferentes, este documento le dará un paso más en algunos filtros de contenido entrantes y salientes muy comunes y recomendados.

Descripción general de los pasos

Paso 1: Importar los diccionarios necesarios

Este documento proporcionará los pasos necesarios para implementar algunas Prácticas Recomendadas Filtros de Contenido Entrante y Saliente. Los filtros de contenido que vamos a crear harán referencia a algunos diccionarios, por lo que primero tendremos que importar esos diccionarios. El ESA se envía con los diccionarios y usted simplemente necesita importarlos a la configuración para hacer referencia a ellos en los Filtros de Contenido que crearemos.

Paso 2: Creación de cuarentenas centralizadas

Para la mayor parte de los filtros de contenido, crearemos, estableceremos la "Acción" en Cuarentena del correo electrónico (o una copia del correo electrónico) en cuarentenas personalizadas especificadas (nuevas) y, por lo tanto, necesitamos primero crear esas

cuarentenas en el SMA, ya que este documento asume que ha habilitado cuarentenas PVO centralizadas (políticas, virus y brotes) entre el ESA y SMA.

Paso 3: Crear los filtros de contenido entrante y saliente y aplicar a las políticas

Una vez que hayamos importado los diccionarios y creado las cuarentenas, crearemos los filtros de contenido entrante y los aplicaremos a las políticas de correo entrante y, a continuación, crearemos los filtros de contenido saliente y los aplicaremos a las políticas de correo saliente.

PASO 1: IMPORTANCIA DE LOS DICCIONARIOS NECESARIOS

Importación de los diccionarios a los que nos referiremos en nuestros filtros de contenido:

- En el dispositivo ESA, vaya a **"Políticas de correo > Diccionarios"**
- Haga clic en el botón "**Importar diccionario**" situado en el lado derecho de la página.

Profanidad:

- Seleccione "**Importar desde el directorio de configuración de su dispositivo IronPort**"
- Seleccione "**profanity.txt**" y haga clic en "**Next**".
- Nombre: **Profanidad**
- Haga clic en "**Coincidir palabras completas**" (MUY IMPORTANTE)
- Modificar los términos (añadir nuevos términos o eliminar términos no deseados)
- Haga clic en "**Enviar**"

Contenido sexual:

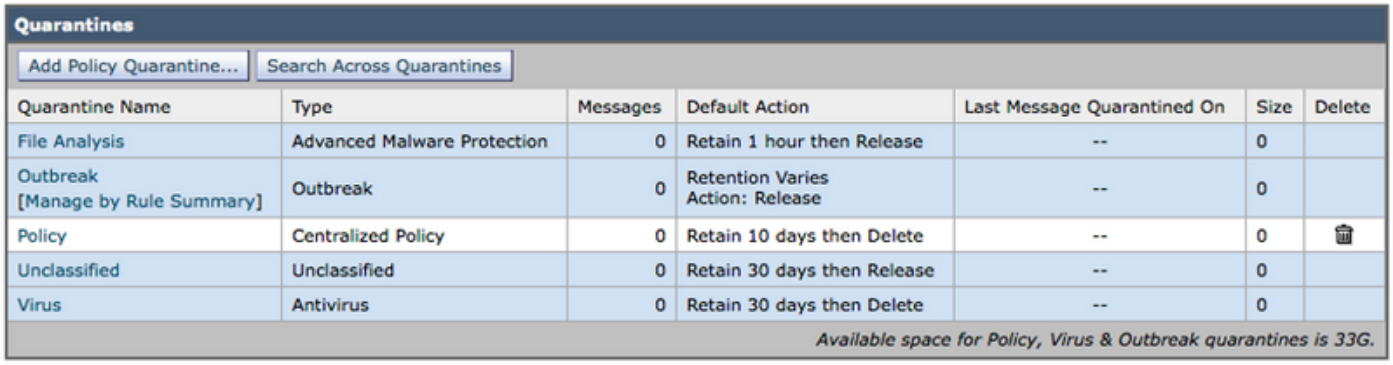
- Seleccione "**Importar desde el directorio de configuración de su dispositivo IronPort**"
- Seleccione "**sexual_content.txt**" y haga clic en "**Siguiente**".
- Nombre: **SexualContent**
- Haga clic en "**Coincidir palabras completas**" (MUY IMPORTANTE)
- Modificar los términos (añadir nuevos términos o eliminar términos no deseados)
- Haga clic en "**Enviar**"

Propiedad:

- Seleccione "**Importar desde el directorio de configuración de su dispositivo IronPort**"
- Seleccione "**owner_content.txt**" y haga clic en "**Next**".
- Nombre: **Propiedad**
- Haga clic en "**Coincidir palabras completas**" (MUY IMPORTANTE)
- Modificar los términos (añadir nuevos términos o eliminar términos no deseados)
- Haga clic en **"Enviar"**

PASO 2: CREACIÓN DE CUARENTENAS CENTRALIZADAS

- En el SMA, vaya a **"Ficha Correo electrónico > Cuarentena de mensajes > Cuarentenas de PVO"**
- Así debe ser la tabla de cuarentenas antes de comenzar. Todas las cuarentenas son predeterminadas.



- Haga clic en el **"Agregar cuarentena de políticas..."** botón
- Cree las siguientes cuarentenas.
- Algunos serán utilizados por filtros de contenido entrante y otros serán utilizados por filtros de contenido saliente. Los crea de la misma manera.

Cuarentenas de PVO: utilizadas por filtros de contenido entrante

Entrada malintencionada de URL:
Nombre: Entrada malintencionada de URL
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Categoría de URL entrante:
Nombre: Categoría de URL entrante
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Datos bancarios entrantes:
Nombre: Datos bancarios entrantes
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Entrante de SSN:
Nombre: SSN entrante
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Entrada inapropiada:
Nombre: Entrante Inapropiado
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Fallo duro de SPF:
Nombre: Falla de SPF
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Fallo de software SPF:
Nombre: Falla de software SPF
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

SpoofMail:
Nombre: SpoofMail
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Fallo duro de DKIM:
Nombre: DKIM Hard Fail
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Entrada protegida por contraseña:
Nombre: Pwd Protected Inbound
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Cuarentenas de PVO: utilizadas por filtros de contenido saliente

Datos bancarios salientes:
Nombre: Datos bancarios salientes
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

SSN saliente:
Nombre: SSN saliente
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Saliente inapropiado:

URL saliente malintencionado:
Nombre: URL malicioso saliente
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Categoría de URL saliente:
Nombre: Categoría de URL saliente
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Saliente protegida por contraseña:

Nombre: Saliente inapropiado
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Nombre: Pwd Protected Outbound
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

Saliente de propiedad:
Nombre: Saliente propiedad
Período de retención: 14 días
Acción predeterminada: Eliminar
Espacio libre: Habilitar

- Esta es la forma en la que su tabla PVO debe cuidar después de crear todas las cuarentenas 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.

PASO 3: CREACIÓN DE LOS FILTROS DE CONTENIDO ENTRANTES

Una vez importados los diccionarios y creadas las cuarentenas de PVO, ahora puede comenzar a crear los filtros de contenido entrante:

- Vaya a: **"Políticas de correo > Filtros de contenido entrante"**
- Esta es una tabla de filtros de contenido entrante que debe crear. Por ejemplo, debajo de la tabla hay una captura de pantalla que muestra cómo crear la primera.

Crear estos filtros de contenido entrante

Nombre: **Datos_bancarios**
Agregar dos condiciones:
Cuerpo o adjunto del mensaje:
Contiene identificador inteligente: Número de routing ABA
Contiene identificador inteligente: Número de tarjeta de crédito
Agregar una acción:

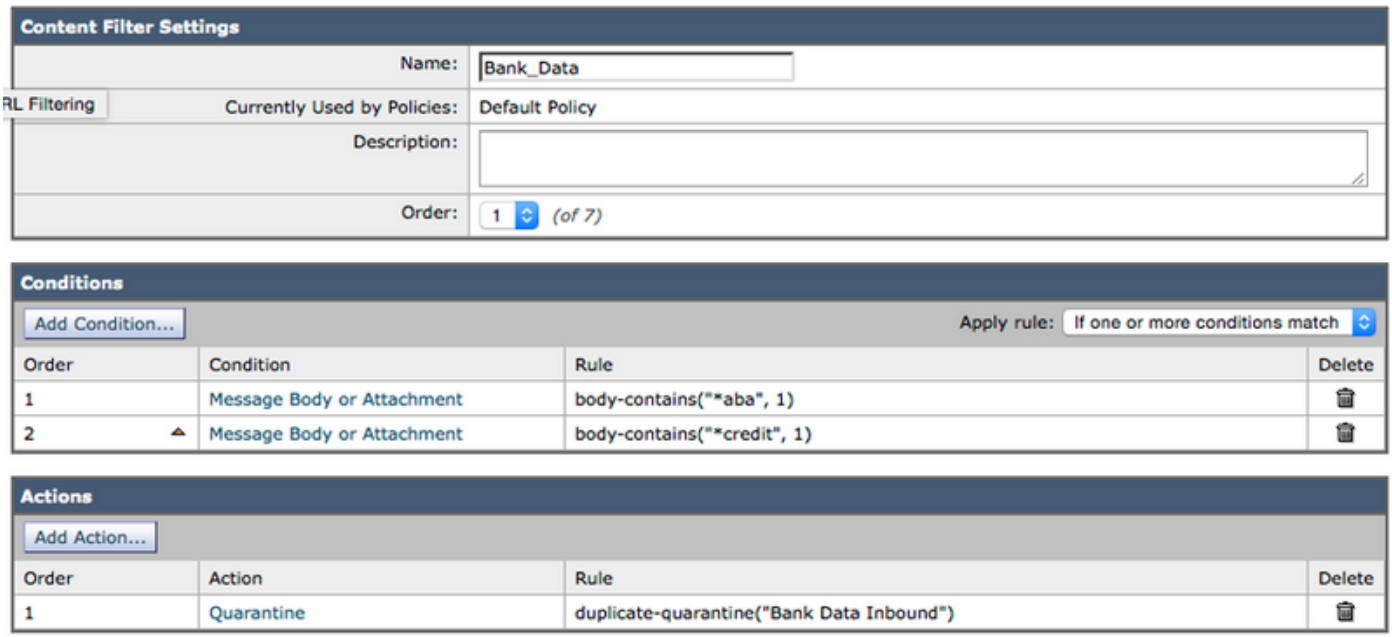
Cuarentena:
Enviar mensaje a cuarentena: "Datos bancarios entrantes (centralizados)"
Mensaje duplicado: Habilitado
(Tenga en cuenta que la regla de aplicación debe ser "Si una o más condiciones coinciden")

Nombre: **SSN**
Agregar una condición:
Cuerpo o adjunto del mensaje:
Contiene identificador inteligente: Número de seguridad social (SSN)
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "SSN entrante (centralizado)"
Mensaje duplicado: Habilitado
Nombre: **Inapropiado**
Agregar dos condiciones:
Cuerpo o adjunto del mensaje:
Contiene un término en el diccionario: Blasfemia
Contiene un término en el diccionario: Contenido sexual
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "Entrante inapropiado (centralizado)"
Mensaje duplicado: Habilitado
Nombre: **URL_Category**
Agregar una condición:
Categoría de URL:
Seleccionar categorías:
Adultos, citas, prevención de filtros, freeware y Shareware, juegos,
Juegos, hackeo, lencería y trajes de baño, desnudez no sexual,
Dominios aparcados, Transferencia de archivos de pares, pornografía
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "Categoría de URL entrante (centralizada)"
Mensaje duplicado: Habilitado
(Nota: Este filtro de contenido requiere que active "Servicios de seguridad"—> "Filtrado de URL")
Nombre: **URL_Malicious**
Agregar una condición:
Reputación de URL:
La reputación de URL es: Malintencionado (-10.0 a -6.0)
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "URL malicioso entrante (centralizado)"
Mensaje duplicado: Desactivado (**** Cuarentena del original ****)
Nombre: **Password_Protected**
Agregar una condición:
Protección de archivos adjuntos: Uno o más adjuntos están protegidos
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "Pwd Protected Inbound (Centralizado)"
Mensaje duplicado: Habilitado

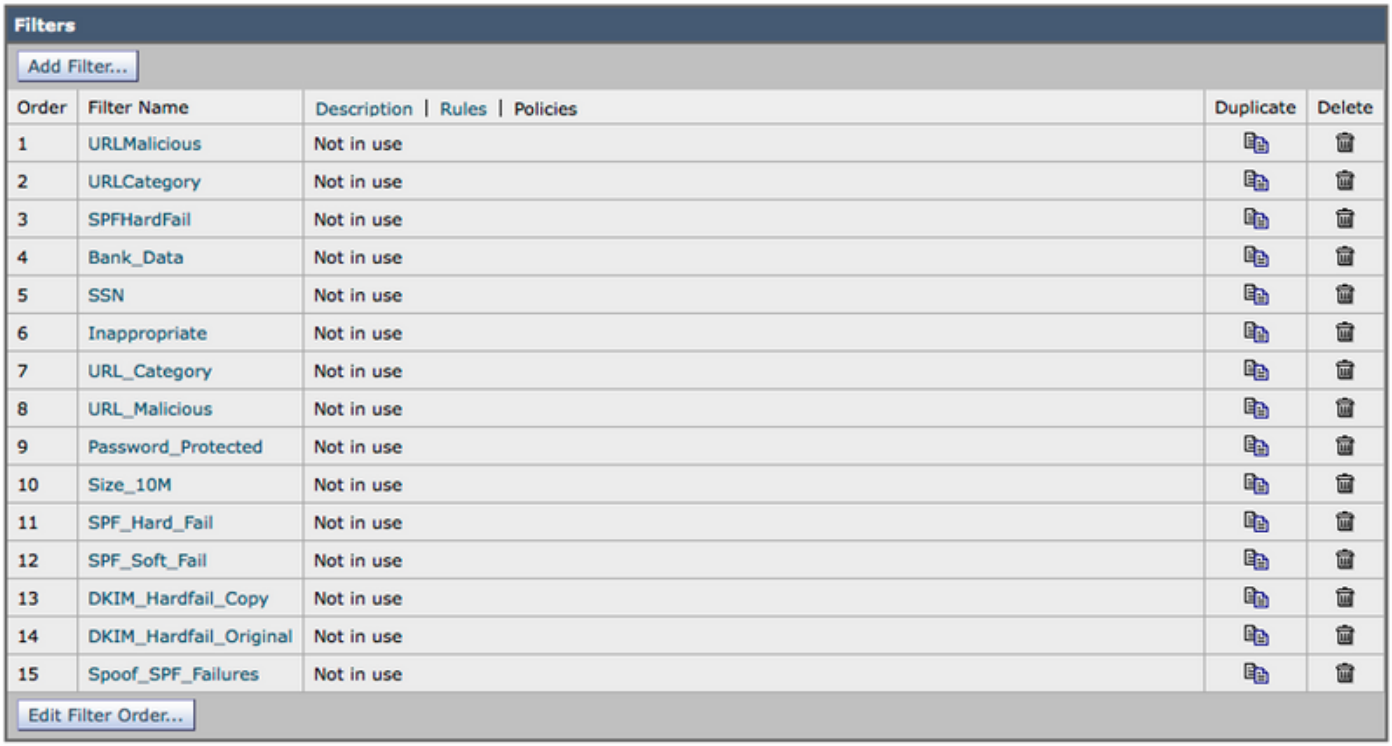
Nombre: **Size_10M**
Agregar una condición:
  El tamaño del mensaje es:
    Mayor o igual que: 10 millones
Agregar una acción:
  Agregar etiqueta de mensaje:
    Introduzca un término: NOOP
(Nota: Debe haber alguna acción, así que aquí "etiquetamos" el mensaje para que no se realice ninguna operación. El hecho de que el filtro de contenido haya sido "Coincidido" le permitirá aparecer en los informes. No es necesario adoptar ninguna "medida" para que aparezca en Reporting.)
Nombre: **SPF_Hard_Fail**
Agregar una condición:
  Verificación SPF: Fallo "es"
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "Fallo de hardware SPF (centralizado)"
    Mensaje duplicado: Habilitado
(Nota: "is Fail" es una falla del SPF duro y significa que el propietario del dominio le está diciendo que descarte todos los correos electrónicos recibidos de remitentes que no están enumerados en su registro SPF. Inicialmente, es una buena idea utilizar "Duplicar mensaje" y revisar las fallas durante una o dos semanas antes de poner en cuarentena el original (es decir, desactivar el mensaje duplicado).
Nombre: **SPF_Soft_Fail**
Agregar una condición:
  Verificación SPF: "is" Softfail
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "Fallo de software SPF (centralizado)"
    Mensaje duplicado: Habilitado
Nombre: **DKIM_Hardfail_Copy**
Agregar una condición:
  Autenticación DKIM: "es" Hardfail
Agregar dos acciones:
  Agregar/Editar encabezado:
    Nombre del encabezado: Asunto
    Haga clic en "Anteponer al valor del encabezado existente" e introduzca: [Copiar - No liberar]"
  Cuarentena:
    Enviar mensaje a cuarentena: "DKIM Hard Fail (centralizado)"
    Mensaje duplicado: Habilitado
(Nota: Poner en cuarentena inicialmente una copia del mensaje).
Nombre: **DKIM_Hardfail_Original**
Agregar una condición:
  Autenticación DKIM: "es" Hardfail
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "DKIM Hard Fail (centralizado)"
    Mensaje duplicado: Inhabilitado
(Nota: Vamos a crear otra fila de política de correo entrante para dominios PayPal y eBay y usaremos este filtro de contenido para dominios que sabemos que deben pasar la verificación DKIM.)
Nombre: **Spoof_SPF_Failure**

Agregue una condición pero tiene ambas opciones: Softfail y Hardfail verificadas:
Verificación SPF: "es" Softfail y haga clic en "Fail" (Fallo)
(por lo que tiene dos casillas de verificación en "Softfail" y "Fail"
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "SpoofMail (centralizado)"
Mensaje duplicado: Habilitar
(Nota: Utilizaremos este filtro de contenido para tomar medidas en el correo electrónico entrante que pretende enviar desde su propio dominio: suplantación. Comience con la acción establecida para poner en cuarentena una copia y después de un par de semanas de revisar la cuarentena de SpoofMail, puede modificar su registro DNS de SPF TXT para agregar todos los remitentes legítimos y, en algún momento, puede cambiar este filtro de contenido para poner en cuarentena el original desactivando la casilla de verificación de mensaje duplicado.)

A modo de ejemplo, así debe ser el filtro de contenido de Bank_Data antes de enviarlo.



Después de crear todos los filtros de contenido entrante, la tabla debe verse de la siguiente manera:



Debido a que la función "Políticas" está seleccionada (verá el hipertexto Políticas en la parte central superior), la columna central muestra las Políticas de correo entrante a las que se ha aplicado el filtro de contenido. Debido a que no los hemos aplicado a ninguna Política de correo entrante, se muestra el mensaje "No en uso".

Aplicar los filtros de contenido entrante a las políticas de correo entrante

- Vaya a: **"Políticas de correo > Políticas de correo entrante"**
- Haga clic en el texto **"Desactivado"** de la celda Filtros de contenido para la **"Política predeterminada"**.
- El botón del menú desplegable se establece en **"Desactivar filtros de contenido"**.
- Haga clic en el botón y establezca en **"Habilitar filtros de contenido"** y se le presentarán inmediatamente todos los filtros de contenido entrante que se hayan creado.
- Habilite todos los filtros excepto DKIM_Hardfail_Original y Spoof_SPF_Failure.
- **"Enviar"** y "**Cometer"**.

Verificación de DKIM para eBay y Paypal y protección de correo electrónico de suplantación para tu dominio

Estos dos temas implicarán filtros de contenido que utilicen la verificación DKIM y la verificación SPF. Por lo tanto, primero debemos garantizar que se habiliten tanto la verificación DKIM como la SPF.

1. Habilitar verificación DKIM y SPF dentro de las políticas de flujo de correo

- Vaya a: **"Políticas de correo > Políticas de flujo de correo"**
- Habilite la verificación de DKIM y SPF en todas las políticas de flujo de correo que tengan "Comportamiento de conexión" de "Aceptar".
- Haga clic en el hipertexto inferior "Default Policy Parameters" y establezca **"DKIM Verification"** en **"On"** y **"SFP/SIDF Verification"**"On".

- Haga clic en **"Enviar"** y **"Confirmar"**.
- Ahora verá la tabla Políticas de flujo de correo. Observe la columna denominada **"Comportamiento"** y edite cualquier política de flujo de correo con el Comportamiento establecido en **"Relay"**
- Active **"Off"** tanto la verificación de DKIM como de SPF para esas políticas de flujo de correo.
- Haga clic en **"Enviar"** y **"Confirmar"**.

No queremos que el ESA realice la verificación de DKIM o SPF para el correo electrónico recibido en el ESA desde el encabezado de Exchange Mail Server saliente. En la mayoría de las configuraciones, la política de flujo de correo "RELAYED" es la única fila con el comportamiento de retransmisión.

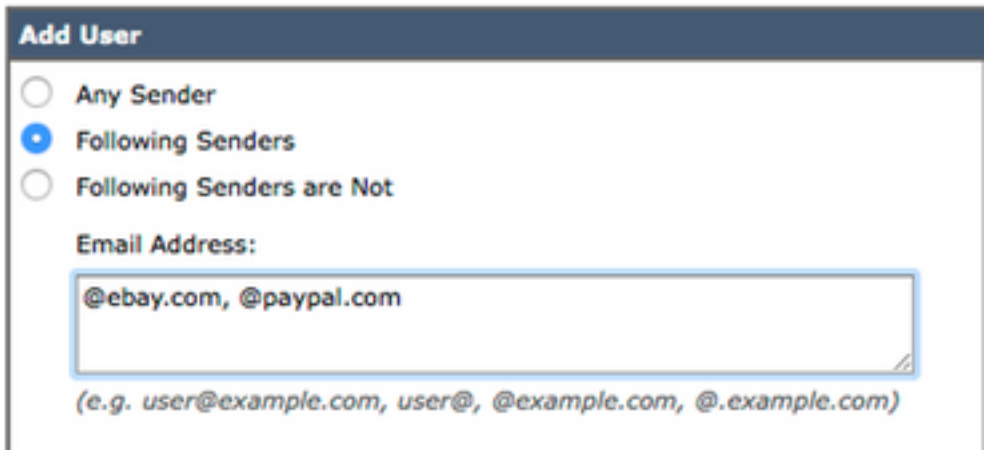
2. Cree una nueva política de flujo de correo entrante para eBay y Paypal

El correo electrónico entrante recibido de eBay y Paypal siempre debe pasar la verificación DKIM. Por lo tanto, crearemos otra política de correo entrante para utilizar el filtro de contenido entrante DKIM_Hardfail_Original para un correo electrónico de esos dominios.

- Vaya a: **"Políticas de correo > Políticas de correo entrante"**
- Haga clic en el botón **"Agregar política"**.
- Introduzca el nombre: **"DKIM Hardfail Original"**
- Haga clic en el **"Agregar usuario..."** para abrir el Navegador.

El siguiente panel de configuración le permite definir qué mensajes coincidirán con esta nueva política de correo entrante. Sólo queremos definir los criterios para el remitente (la parte izquierda del panel de configuración).

- Haga clic **"Siguientes remitentes"** y, en la tabla Direcciones de correo electrónico, escriba **"@ebay.com, @paypal.com"**



- Haga clic en el **“Ok”** en la parte inferior.
- Haga clic **"Enviar"**.

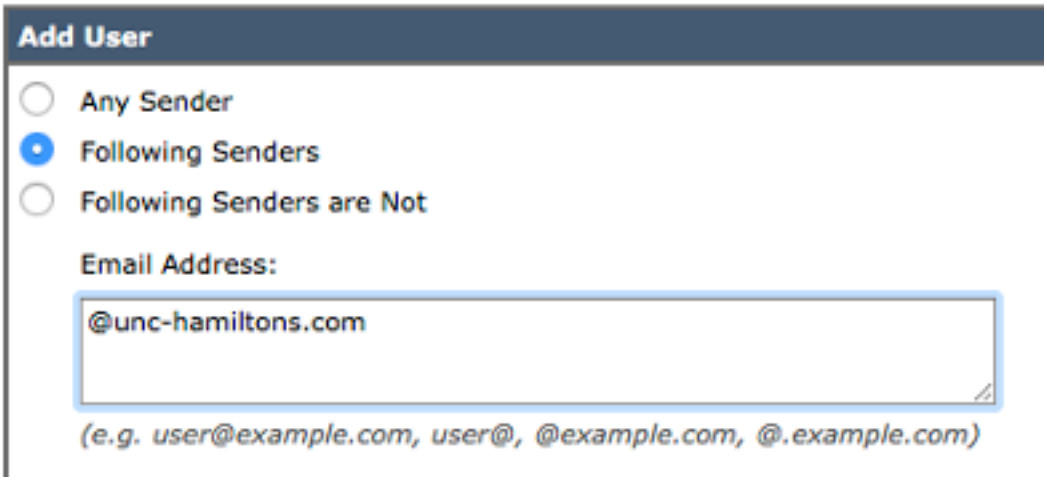
3. Cree una nueva política de flujo de correo entrante para su dominio (protección contra suplantación)

Los pasos de esta sección le permitirán tomar medidas sobre el correo electrónico entrante que tenga una dirección de correo electrónico de origen de su propio dominio y que no esté en condiciones de verificar SPF. Por supuesto, esto depende de que ya haya publicado su registro de texto SPF en DNS. Omita estos pasos si no ha creado/publicado un registro de recursos de texto SPF para su dominio.

- Vaya a: **"Políticas de correo > Políticas de correo entrante"**
- Haga clic en el botón **"Agregar política"**.
- Introduzca el nombre: **"Spoof_Protection"**
- Haga clic en el **"Agregar usuario..."** para abrir el Navegador.

El siguiente panel de configuración le permite definir qué mensajes coincidirán con esta nueva fila de política de correo entrante. Sólo desea definir los criterios para el remitente (que es la parte izquierda del panel de configuración).

- Haga clic en el **"Siguientes remitentes"** y, a continuación, introduzca su dominio en el cuadro de texto **"Dirección de correo electrónico:"**. Para mí, mi dominio es **"@unc-hamiltons.com"**



- Haga clic **"Enviar"**.

Se le vuelve a presentar la tabla Políticas de correo entrante, pero ahora tiene una segunda fila de política de correo nueva por encima de la política predeterminada.

- Haga clic en el hipertexto **(use default)** de la celda Filtros de contenido para la nueva fila.
- Cambie el menú desplegable a **"Habilitar filtros de contenido (configuración personalizada)"**.
- Verifique que **"Spoof_SPF_Failure"** también asegúrese de que tanto "DKIM_Hardfail_Copy" como **"DKIM_Hardfail_Original"** no estén marcados.
- Haga clic en **"Enviar"** y **"Registrar cambios"**.

La tabla Políticas de correo entrante debería verse así:

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	

PASO 4: CREACIÓN DE LOS FILTROS DE CONTENIDO SALIENTES

- Vaya a: **"Políticas de correo > Filtros de contenido saliente"**
- Esta es una tabla de filtros de contenido saliente que debe crear.

Crear estos filtros de contenido saliente

Nombre: **Datos_bancarios**
Agregar dos condiciones:
  Cuerpo o adjunto del mensaje:
    Contiene identificador inteligente: Número de routing ABA
    Contiene identificador inteligente: Número de tarjeta de crédito
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "Datos bancarios salientes (centralizados)"
    Mensaje duplicado: Habilitado
(Tenga en cuenta que la regla de aplicación debe ser "Si una o más condiciones coinciden")
Nombre: **SSN**
Agregar una condición:
  Cuerpo o adjunto del mensaje:
    Contiene identificador inteligente: Número de seguridad social (SSN)
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "SSN saliente (centralizado)"
    Mensaje duplicado: habilitado
Nombre: **Inapropiado**
Agregar dos condiciones:
  Cuerpo o adjunto del mensaje:
    Contiene un término en el diccionario: Blasfemia
    Contiene un término en el diccionario: Contenido sexual
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "Saliente inapropiado (centralizado)"
    Mensaje duplicado: Habilitado
Nombre: **URL_Category**
Agregar una condición:
  Categoría de URL:
    Seleccionar categorías:
      Adultos, citas, prevención de filtros, freeware y Shareware, juegos,
      Juegos, hackeo, lencería y trajes de baño, desnudez no sexual,
      Dominios aparcados, Transferencia de archivos de pares, pornografía
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "Categoría de URL saliente (centralizada)"
    Mensaje duplicado: Habilitado
Nombre: **URL_Malicious**
Agregar una condición:
  Reputación de URL:
    La reputación de URL es: Malintencionado (-10.0 a -6.0)
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "URL malicioso saliente (centralizado)"
    Mensaje duplicado: Desactivado (**** Cuarentena del original ****)
Nombre: **Password_Protected**
Agregar una condición:
  Protección de archivos adjuntos: Uno o más adjuntos están protegidos
Agregar una acción:
  Cuarentena:
    Enviar mensaje a cuarentena: "Pwd Protected Outbound (Centralizado)"

Mensaje duplicado: Habilitado
Nombre: **Size_10M**
Agregar una condición:
El tamaño del mensaje es:
Mayor o igual que: 10 millones
Agregar una acción:
Agregar etiqueta de mensaje:
Introduzca un término: NOOP
(Nota: Debe haber alguna acción, así que aquí "etiquetamos" el mensaje para que no se realice ninguna operación. El hecho de que el filtro de contenido haya sido "Coincidido" le permitirá aparecer en los informes. No es necesario adoptar ninguna "medida" para que aparezca en Reporting.)
Nombre: **Propiedad**
Agregar una condición:
Cuerpo o adjunto del mensaje:
Contiene un término en el diccionario: Propiedad
Agregar una acción:
Cuarentena:
Enviar mensaje a cuarentena: "Propiedad (centralizada)"
Mensaje duplicado: Habilitado

Dado que la función "Políticas" está seleccionada (verá el hipertexto Políticas en la parte central superior), la columna central muestra las Políticas de correo saliente a las que se ha aplicado el filtro de contenido. Puesto que no los hemos aplicado a ninguna política de correo saliente, se muestra el mensaje "No en uso".

- Vaya a: **"Políticas de correo > Políticas de correo saliente"**
- Haga clic en el texto **"Desactivado"** de la celda Filtros de contenido para la política predeterminada.
- El botón del menú desplegable se establece en "**Deshabilitar filtros de contenido**".
- Haga clic en el botón y establezca en **"Habilitar filtros de contenido"** y se le presentarán inmediatamente todos los filtros de contenido saliente que se hayan creado.
- **"Activar"** todos los filtros.
- **"Enviar"** y **"Cometer"**.

Summary

Ya ha implementado las mejores prácticas iniciales para los filtros de contenido entrante y saliente. La mayoría de los filtros de contenido (no todos) utilizaron la acción de cuarentena y eligieron marcar (Habilitar) la "opción Duplicar mensaje", que simplemente coloca una copia del correo electrónico original y no impide que se envíe el correo electrónico. El objetivo de estos filtros de contenido es permitirle recopilar información sobre los tipos de mensajes de correo electrónico entrantes y salientes para su empresa.

Dicho esto, después de ejecutar el informe Filtros de contenido y de ver las copias de correo electrónico guardadas en las cuarentenas, puede ser prudente desmarcar la opción de casilla de verificación "Duplicar mensaje" y así empezar a poner el correo electrónico original en la cuarentena en lugar de una copia/duplicado.