Configuración de Cloud Gateway Gold

Contenido

Introducción

Este documento describe un análisis en profundidad de la configuración Gold proporcionada para Cisco Secure Email Cloud Gateway. La configuración Gold para clientes en la nube de Cisco Secure Email es la práctica recomendada y la configuración de día cero tanto para el Cloud Gateway como para Cisco Secure Email and Web Manager. Las implementaciones de Cisco Secure Email Cloud utilizan tanto gateways de nube como al menos un (1) gestor de correo electrónico y web. Algunas partes de la configuración y de las prácticas recomendadas indican a los administradores que utilicen las cuarentenas que se encuentran en el Email and Web Manager con fines de administración centralizada.

Prerequisites

Requirements

Cisco recomienda que conozca estos temas:

- Cisco Secure Email Gateway o Cloud Gateway, administración de UI y CLI
- Cisco Secure Email and Web Manager, administración a nivel de interfaz de usuario
- Los clientes de Cisco Secure Email Cloud pueden solicitar acceso a CLI; consulte: Acceso a la interfaz de línea de comandos (CLI)

Componentes Utilizados

La información de este documento procede de la configuración gold y de las recomendaciones de prácticas recomendadas para los clientes y administradores de Cisco Secure Email Cloud.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Productos Relacionados

Este documento también es aplicable con:

- Hardware o dispositivo virtual de Cisco Secure Email Gateway en las instalaciones
- Dispositivo virtual y hardware en las instalaciones de Cisco Secure Email and Web Manager

Cuarentenas de políticas

Las cuarentenas se configuran y se mantienen en el Email and Web Manager para los clientes de Cisco Secure Email Cloud. Inicie sesión en su Email and Web Manager para ver las cuarentenas:

- ACCOUNT_TAKEOVER
- ANTI_SPOOF
- BLOCK_ATTACHMENTS
- LISTA DE BLOQUEO
- DKIM_FAIL
- CUARENTENA_DMARC
- DMARC_REJECT
- CORREO_FORJADO
- INAPPROPRIATE_CONTENT
- MACRO

- OPEN_RELAY
- SDR_DATA
- SPF_HARDFAIL
- SPF_SOFTFAIL
- TG_OUTBOUND_MALWARE
- URL_MALINTENCIONADO

Configuración Gold de gateway de nube

> **Advertencia**: cualquier cambio en las configuraciones basado en las prácticas recomendadas que se proporcionan en este documento debe revisarse y entenderse antes de aplicar los cambios de configuración en su entorno de producción. Póngase en contacto con su ingeniero de Cisco CX, su gerente de servicios designado (DSM) o su equipo de cuentas antes de realizar cambios en la configuración.

Configuración Básica

Políticas de correo > Tabla de acceso de destinatarios (RAT)

La Tabla de Acceso de Destinatarios define qué destinatarios son aceptados por un receptor público. Como mínimo, la tabla especifica la dirección y si se debe aceptar o rechazar. Revise la RAT para agregar y administrar los dominios según sea necesario.

Red > Rutas SMTP

Si el destino de la ruta SMTP es Microsoft 365, vea Office365 Throttling CES New Instance with "4.7.500 Server busy. Intente nuevamente más tarde.

Servicios de seguridad

Los servicios enumerados se configuran para todos los clientes de Cisco Secure Email Cloud con los valores proporcionados:

IronPort Anti-Spam (IPAS)

- Activado y configurado: analizar siempre 1M y no analizar nunca 2M
- Tiempo de espera para analizar un solo mensaje: 60 segundos

Filtrado de URL

- Habilitar categorización de URL y filtros de reputación
- (Opcional) Cree y configure la lista de permitidos de URL denominada "bypass_urls".

- Habilitar seguimiento de interacción web
- Configuración avanzada: Límite de tiempo de búsqueda de URL: 15 segundosNúmero máximo de URL escaneadas en el cuerpo y el adjunto: 400Reescriba el texto de la dirección URL y HREF en el mensaje: NoRegistro de URL: Habilitado
- (Opcional) A partir de AsyncOS 14.2 para Cloud Gateway, están disponibles Veredicto retrospectivo de URL y Remediación de URL; consulte las notas de la versión proporcionadas y Configure URL Filtering for Secure Email Gateway and Cloud Gateway

Detección de graymail

- Activar y configurar Explorar siempre 1M y No explorar nunca 2M
- Tiempo de espera para analizar un solo mensaje: 60 segundos

Filtros de brote

- Habilitar reglas adaptables
- Tamaño máximo de mensaje a analizar: 2 millones
- Habilitar seguimiento de interacción web

Protección frente a malware avanzado > Reputación y análisis de archivos

- Habilitar Reputación de archivos
- Habilitar análisis de archivos Consulte la configuración global para revisar los tipos de archivos para el análisis de archivos

Rastreo de mensajes

- Activar registro de conexiones rechazadas (si es necesario)

Administración del sistema

Usuarios (Administración del sistema > Usuarios)

- Recuerde revisar y establecer las políticas de frase de contraseña asociadas con la **configuración de cuenta de usuario local y frase de contraseña**
- Si es posible, configure y habilite el protocolo ligero de acceso a directorios (LDAP) para la autenticación (**Administración del sistema > LDAP**)

Suscripciones de registro (Administración del sistema > Suscripciones de registro)

- Si no está configurado, cree y habilite: Registros del historial de configuraciónRegistros del cliente de reputación de URL
- En Configuración global de suscripciones a registros, edite la configuración y agregue los encabezados **To**, **From**, **Reply-To**, **Sender**.

Configuración adicional (opcional)

Servicios adicionales para revisar y considerar:

Administración del sistema > LDAP

- Si configura LDAP, Cisco recomienda LDAP con SSL habilitado

Defensa de URL

- Consulte Configuración del filtrado de URL para Secure Email Gateway y Cloud Gateway para obtener las prácticas recomendadas de configuración más actualizadas para la defensa de URL.
- Cisco también profundiza en la defensa de URL; consulte la Guía de defensa de URL.
- En este documento también se incluyen algunos ejemplos incluidos en la Guía de defensa de URL.

SPF

- Los registros DNS del marco de políticas de remitente (SPF) se crean externamente en el gateway de la nube. Por lo tanto, Cisco recomienda encarecidamente a todos los clientes que integren las prácticas recomendadas de SPF, DKIM y DMARC en su estrategia de seguridad. Consulte Configuración y prácticas recomendadas de SPF para obtener más información sobre la validación de SPF.
- Para los clientes de Cisco Secure Email Cloud, se publica una macro para todas las puertas de enlace de la nube por nombre de host de asignación para facilitar la adición de todos los hosts.
- Colóquelo antes de ~all o -all dentro del registro DNS TXT (SPF) actual, si existe:

```
exists:%{i}.spf.<allocation>.iphmx.com
```

> **Nota**: Asegúrese de que el registro SPF finaliza con **~all** o **-all**. Valide los registros SPF de sus dominios antes y después de cualquier cambio.

- Información y herramientas recomendadas para obtener más información sobre SPF: SPF Record Checker - Búsqueda de SPF gratuita (dmarcian.com)Tabla de sintaxis de registro SPF - Todo SPF - dmarcian.com

Ejemplos adicionales de SPF

- Un excelente ejemplo de SPF es si recibe mensajes de correo electrónico desde el gateway de la nube y envía mensajes de correo electrónico salientes desde otros servidores de correo. Puede utilizar el mecanismo "a:" para especificar hosts de correo:

```
v=spf1 mx a:mail01.yourdomain.com a:mail99.yourdomain.com ~all
```

- Si solo envía mensajes de correo electrónico salientes a través del gateway de la nube, puede utilizar:

```
v=spf1 mx exists:%{i}.spf.<allocation>.iphmx.com ~all
```

- En este ejemplo, el mecanismo "ip4:" o "ip6:" especifica una dirección IP o un rango de direcciones IP:

```
v=spf1 exists:%{i}.spf.<allocation>.iphmx.com ip4:192.168.0.1/16 ~all
```

Cambios de nivel de CLI

- Como se indica en Requisitos previos, los clientes de Cisco Secure Email Cloud pueden solicitar acceso a CLI; consulte Acceso a la interfaz de línea de comandos (CLI).

Filtro anti-simulación

- Asegúrese de revisar la Guía de prácticas recomendadas para la lucha contra la suplantación
- Esta guía le proporciona ejemplos detallados y prácticas recomendadas de configuración para la prevención de suplantación de correo electrónico

Agregar filtro de encabezado

- Solo CLI, escriba y habilite el filtro de mensajes addHeaders:

```
addHeaders:  if (sendergroup != "RELAYLIST")
{
    insert-header("X-IronPort-RemoteIP", "$RemoteIP");
    insert-header("X-IronPort-MID", "$MID");
    insert-header("X-IronPort-Reputation", "$Reputation");
    insert-header("X-IronPort-Listener", "$RecvListener");
    insert-header("X-IronPort-SenderGroup", "$Group");
    insert-header("X-IronPort-MailFlowPolicy", "$Policy");
}
```

Tabla de acceso de host (Políticas de correo > Tabla de acceso de host (HAT))

Descripción General de HAT > Grupos de Remitentes Adicionales

- Guía del usuario de ESA: creación de un grupo de remitentes para la gestión de mensajes BYPASS_SBRS - Colocar más alto para fuentes que omiten la reputaciónMY_TRUSTED_SPOOF_HOSTS - Parte del filtro de suplantaciónTLS_REQUIRED: para conexiones TLS forzadas

En el grupo de remitentes SUSPECTLIST predefinido

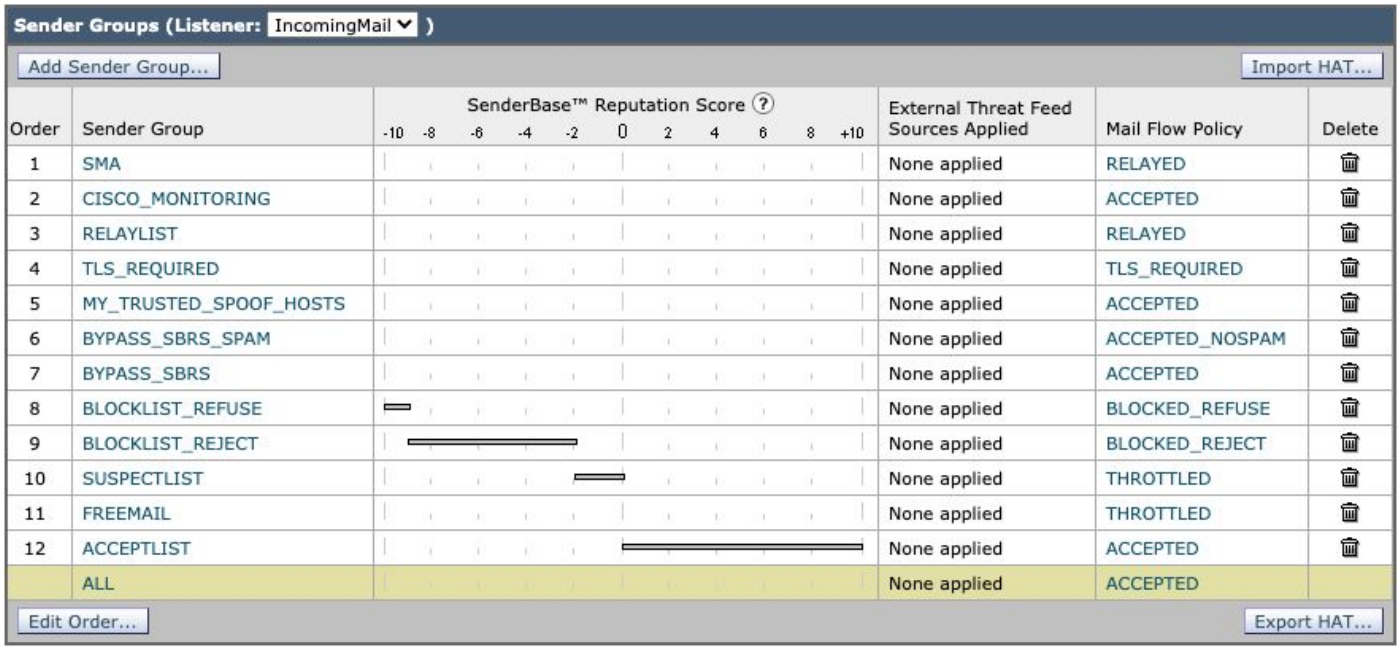
- Guía del usuario de ESA: Verificación de remitente: Host active "Puntuaciones SBRS en Ninguna".(Opcional) habilitar "Error de búsqueda de registros PTR del host de conexión debido a un error temporal de DNS".

Ejemplo de HAT agresivo

- BLOCKLIST_REFUSE [-10.0 a -9.0] POLÍTICA: BLOCKED_REFUSE
- BLOCKLIST_REJECT [-9.0 a -2.0] POLÍTICA: BLOCKED_REJECT
- SUSPECTLIST [-2.0 a 0.0 y puntuaciones SBRS de "None"] POLÍTICA: ACELERADO
- ACCEPTLIST [0.0 to 10.0] POLÍTICA: ACEPTADO

Nota: Los ejemplos de HAT muestran políticas de flujo de correo (MFP) configuradas adicionalmente. Para obtener información completa sobre MFP, consulte "Introducción a la canalización de correo electrónico > Entrantes/Receptores" en la Guía del usuario para obtener la versión adecuada de AsyncOS para Cisco Secure Email Gateway que ha implementado.

Ejemplo de HAT:



Sender Groups (Listener: IncomingMail)

Add Sender Group... | Import HAT...

Order	Sender Group	SenderBase™ Reputation Score -10 -8 -6 -4 -2 0 2 4 6 8 +10	External Threat Feed Sources Applied	Mail Flow Policy	Delete
1	SMA		None applied	RELAYED	
2	CISCO_MONITORING		None applied	ACCEPTED	
3	RELAYLIST		None applied	RELAYED	
4	TLS_REQUIRED		None applied	TLS_REQUIRED	
5	MY_TRUSTED_SPOOF_HOSTS		None applied	ACCEPTED	
6	BYPASS_SBRS_SPAM		None applied	ACCEPTED_NOSPAM	
7	BYPASS_SBRS		None applied	ACCEPTED	
8	BLOCKLIST_REFUSE		None applied	BLOCKED_REFUSE	
9	BLOCKLIST_REJECT		None applied	BLOCKED_REJECT	
10	SUSPECTLIST		None applied	THROTTLED	
11	FREEMAIL		None applied	THROTTLED	
12	ACCEPTLIST		None applied	ACCEPTED	
	ALL		None applied	ACCEPTED	

Edit Order... | Export HAT...

Política de flujo de correo (parámetros de política predeterminados)

Parámetros de política predeterminados

Configuración de seguridad

- Establecer Seguridad de la capa de transporte (TLS) como preferida
- Habilitar el marco de directivas de remitentes (SPF)
- Habilitar DomainKeys Identified Mail (DKIM)
- Habilitar la verificación de autenticación de mensajes, informes y conformidad basada en dominio (DMARC) y enviar informes de comentarios agregados

Nota: DMARC requiere ajustes adicionales para su configuración. Para obtener más información sobre DMARC, consulte "Autenticación de correo electrónico > Verificación de DMARC" en la guía del usuario para obtener la versión adecuada de AsyncOS para Cisco Secure Email Gateway que ha implementado.

Políticas de correo entrante

La política predeterminada está configurada de manera similar a:

Anti-Spam

- Habilitado, con umbrales dejados en los umbrales predeterminados. (La modificación de la puntuación podría aumentar los falsos positivos.)

Antivirus

- Escaneo de mensajes: **buscar virus solamente** Se ha activado la casilla de verificación Asegurar para "Incluir un X-encabezado"
- Para **Mensajes no escaneables** y **Mensajes infectados por virus**, establezca **Archivar mensaje original** en **No**

AMP

- Para **Acciones no escaneables en Errores de Mensaje**, utilice **Avanzado** y **Agregar Encabezado Personalizado al Mensaje**, X-TG-MSGERROR, valor: Verdadero.
- Para las **acciones no escaneables en el límite de velocidad**, utilice **Advanced** y **Add Custom Header to Message**, X-TG-RATELIMIT, value: Verdadero.
- Para **Mensajes con Análisis de Archivo Pendiente**, utilice **Acción Aplicada al Mensaje**: "Cuarentena."

Graymail

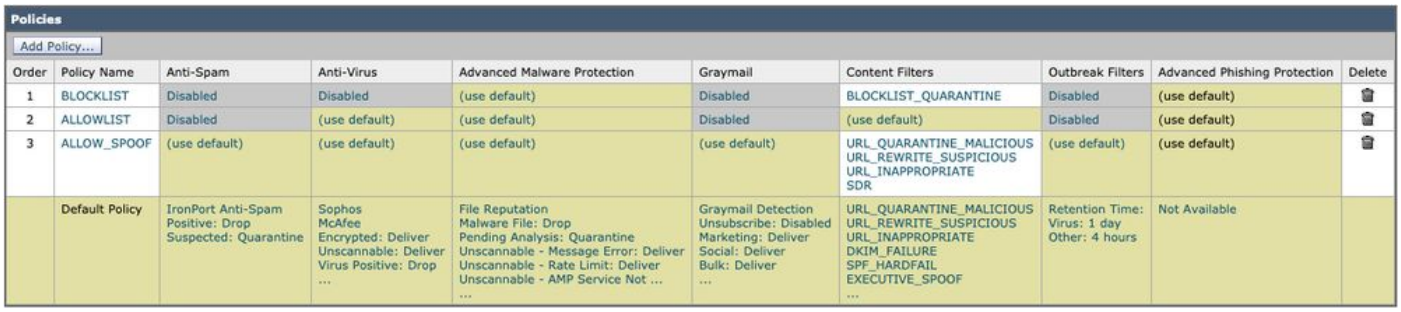
- El escaneo está habilitado para cada veredicto (marketing, redes sociales, en masa), con **Prepend** para **Add Text to Subject** y action es **Deliver**.
- Para **Acción en Bulk Mail**, utilice **Advanced** y **Add Custom Header (opcional)**: X-Bulk, valor: Verdadero.

Filtros de contenido

- Enabled y URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE_SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT están seleccionados
- Estos filtros de contenido se proporcionan más adelante en esta guía

Filtros de brote

- El nivel de amenaza predeterminado es 3; por favor, ajústese a sus requisitos de seguridad. Si el nivel de amenaza de un mensaje es igual o superior a este umbral, el mensaje se traslada a la cuarentena de Outbreak. (1=amenaza más baja, 5=amenaza más alta)
- Habilitar modificación del mensaje
- Reescritura de URL establecida en "Habilitar para todos los mensajes".
- Cambiar asunto anteponer a: [Posible fraude de $threat_category]



Policies

Add Policy...

Order	Policy Name	Anti-Spam	Anti-Virus	Advanced Malware Protection	Graymail	Content Filters	Outbreak Filters	Advanced Phishing Protection	Delete
1	BLOCKLIST	Disabled	Disabled	(use default)	Disabled	BLOCKLIST_QUARANTINE	Disabled	(use default)	
2	ALLOWLIST	Disabled	(use default)	(use default)	Disabled	(use default)	Disabled	(use default)	
3	ALLOW_SPOOF	(use default)	(use default)	(use default)	(use default)	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE SDR	(use default)	(use default)	
	Default Policy	IronPort Anti-Spam Positive: Drop Suspected: Quarantine	Sophos McAfee Encrypted: Deliver Unscannable: Deliver Virus Positive: Drop ...	File Reputation Malware File: Drop Pending Analysis: Quarantine Unscannable - Message Error: Deliver Unscannable - Rate Limit: Deliver Unscannable - AMP Service Not	Graymail Detection Unsubscribe: Disabled Marketing: Deliver Social: Deliver Bulk: Deliver ...	URL_QUARANTINE_MALICIOUS URL_REWRITE_SUSPICIOUS URL_INAPPROPRIATE DKIM_FAILURE SPF_HARDFAIL EXECUTIVE_SPOOF ...	Retention Time: Virus: 1 day Other: 4 hours	Not Available	

Nombres de políticas (mostrado)

- **Política de correo BLOCKLIST**
  La política de correo BLOCKLIST se configura con todos los servicios desactivados, excepto la protección frente a malware avanzado, y enlaza a un filtro de contenido con la acción de QUARANTINE.

- **Política de correo ALLOWLIST**
  La política de correo ALLOWLIST tiene antispam, graymail deshabilitado y filtros de contenido habilitados para URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, DKIM_FAILURE, SPF_HARDFAIL, EXECUTIVE SPOOF, DOMAIN_SPOOF, SDR, TG_RATE_LIMIT o filtros de contenido de su elección y configuración.

- **Política de correo ALLOW_SPOOF**
  La política de correo ALLOW_SPOOF tiene todos los servicios predeterminados habilitados, con los filtros de contenido habilitados para URL_QUARANTINE_MALICIOUS, URL_REWRITE_SUSPICIOUS, URL_INAPPROPRIATE, SDR o los filtros de contenido de su elección y configuración.

Políticas de correo saliente

La política predeterminada está configurada de manera similar a:

Anti-Spam

- Inhabilitado

Antivirus

- Análisis de mensajes: **Buscar sólo virus** Desactive la casilla de verificación "Incluir un encabezado X".
- (Opcional) Para todos los mensajes: **Avanzado > Otra notificación**, active "Otros" e incluya su dirección de correo electrónico de contacto de administración/SOC

Protección frente a malware avanzado

- Habilitar sólo Reputación de archivos
- **Acciones no escaneables en el límite de velocidad**: utilice **Advanced** y **Add Custom Header to Message**: X-TG-RATELIMIT, valor: "Cierto".

- **Mensajes con archivos adjuntos de malware**: utilice **Advanced** y **Add Custom Header to Message**: X-TG-OUTBOUND, valor: "MALWARE DETECTADO".

Graymail

- Inhabilitado

Filtros de contenido

- Se seleccionan los filtros Enabled y TG_OUTBOUND_MALICIOUS, Strip_Secret_Header, EXTERNAL_SENDER_REMOVE, ACCOUNT_TAKEOVER o de contenido que desee.

Filtros de brote

- Inhabilitado

DLP

- Habilitación, según la licencia de DLP y la configuración de DLP.

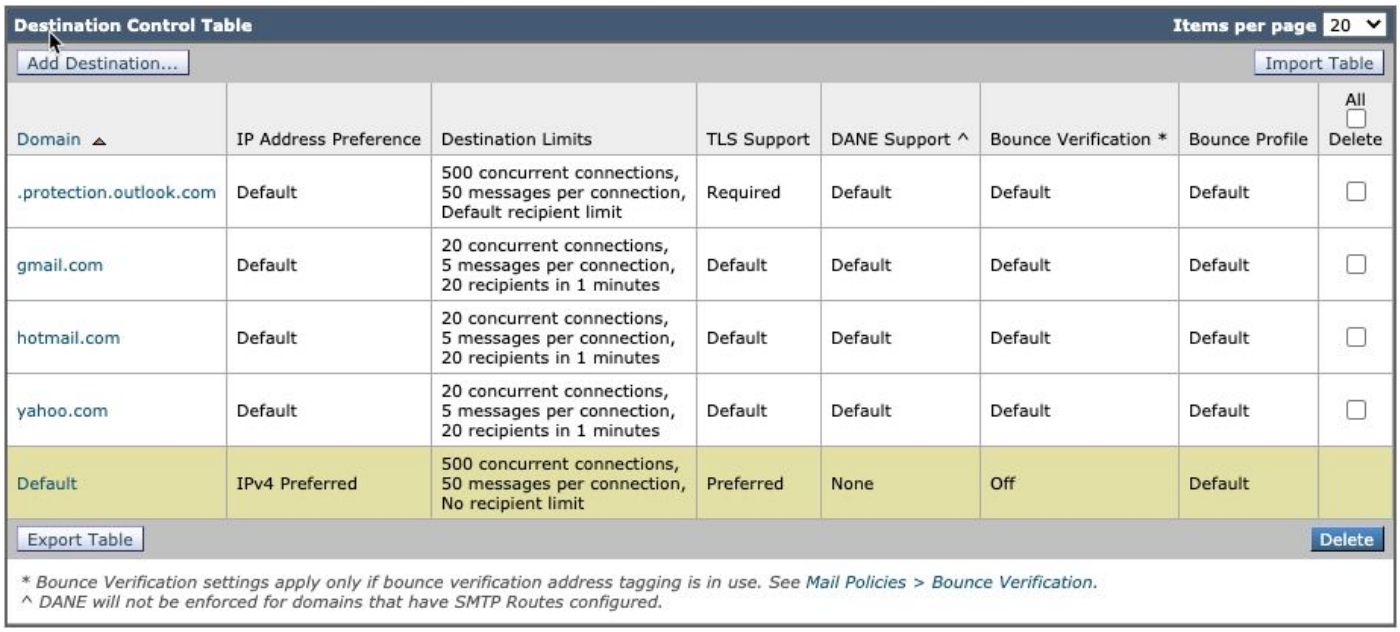
Otros parámetros

Diccionarios (Políticas de correo > Diccionarios)

- Habilitar y revisar **Profanity** y el diccionario **Sexual_Content**
- Cree el diccionario **Executive_FED** para la detección de correo electrónico falsificado con todos los nombres de ejecutivos
- Cree diccionarios adicionales para palabras clave restringidas o de otro tipo según considere necesario para sus políticas, entorno y control de seguridad

Controles de destino (Políticas de correo > Controles de destino)

- Para el dominio predeterminado, configure **TLS Support** como **Preferred**.
- Puede agregar destinos para dominios de correo web y establecer umbrales más bajos
- Consulte nuestra guía Rate Limit Your Outbound Mail with Destination Control Settings para obtener más información.



Destination Control Table — Items per page: 20

Add Destination... | Import Table

Domain	IP Address Preference	Destination Limits	TLS Support	DANE Support ^	Bounce Verification *	Bounce Profile	All Delete
.protection.outlook.com	Default	500 concurrent connections, 50 messages per connection, Default recipient limit	Required	Default	Default	Default	
gmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
hotmail.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
yahoo.com	Default	20 concurrent connections, 5 messages per connection, 20 recipients in 1 minutes	Default	Default	Default	Default	
Default	IPv4 Preferred	500 concurrent connections, 50 messages per connection, No recipient limit	Preferred	None	Off	Default	

Export Table | Delete

** Bounce Verification settings apply only if bounce verification address tagging is in use. See Mail Policies > Bounce Verification.*
^ DANE will not be enforced for domains that have SMTP Routes configured.

Filtros de contenido

> **Nota:** Para obtener información adicional sobre los filtros de contenido, consulte "Filtros de contenido" en la guía del usuario para obtener la versión adecuada de AsyncOS para Cisco Secure Email Gateway que ha implementado.

Filtros de contenido entrante

URL_QUARANTINE_MALICIOUS

Condición: Reputación de URL; reputación de URL (-10.00, -6.00 , "bypass_urls", 1, 1)

Acción: Cuarentena: quarantine("URL_MALICIOUS")

URL_REWRITE_SUSPICIOUS

Condición: Reputación de URL; reputación de URL (-5.90, -5.60 , "bypass_urls", 0, 1)

Acción: Reputación de URL; url-reputación-proxy-redirect(-5,90, -5,60,"",0)

URL_INAPROPIADO

Condición: Categoría de URL; url-category (['Adultos', 'Contenido de abuso infantil', 'Extremo', 'Discurso de odio', 'Actividades ilegales', 'Descargas ilegales', 'Drogas ilegales', 'Pornografía', 'Evitación de filtros'], "bypass_urls", 1, 1)

Acción: Cuarentena; duplicate-quarantine("INAPPROPRIATE_CONTENT")

DKIM_FAILURE

Condición: Autenticación DKIM; dkim-authentication == hardfail

Acción: Cuarentena; duplicate-quarantine("DKIM_FAIL")

SPF_HARDFAIL

Condición: Verificación SPF; spf-status == fail

Acción: Cuarentena; duplicate-quarantine("SPF_HARDFAIL")

EXECUTIVE_SPOOF

Condición: Detección de correo electrónico falsificado; detección de correo electrónico falsificado ("Executive_FED", 90, "")

Condición: Otro encabezado; header("X-IronPort-SenderGroup") != "(?i)allowspoof"

* set Aplicar regla: Sólo si todas las condiciones coinciden

Acción: Agregar/editar encabezado; edit-header-text("Asunto", "(.*)", "[EXTERNO]\\1")

Acción: Cuarentena; cuarentena duplicada("FORGED_EMAIL")

DOMAIN_SPOOF

Condición: Otro Encabezado; header("X-Spoof")

Acción: Cuarentena; duplicate-quarantine("ANTI_SPOOF")

SDR

Condición: Reputación de dominio; reputación de SDR (['horrible'], "")

Condición: Reputación de dominio; antigüedad de SDR ("días", <, 5, "")

* set **Aplicar regla: Si una o más condiciones coinciden**

Acción: Cuarentena; duplicate-quarantine("SDR_DATA")

TG_RATE_LIMIT

Condición: Otro encabezado; header("X-TG-RATELIMIT")

Acción: Add Log Entry; log-entry("X-TG-RATELIMIT: $filenames")

BLOCKLIST_QUARANTINE

Condición: (Ninguno)

Acción: Cuarentena; quarantine("BLOCKLIST")

Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	URL_QUARANTINE_MALICIOUS	URL_QUARANTINE_MALICIOUS: if (url-reputation(-10.00, -6.00 , "bypass_urls", 1, 1)) { quarantine("URL_MALICIOUS"); }		
2	URL_REWRITE_SUSPICIOUS	URL_REWRITE_SUSPICIOUS: if (url-reputation(-5.90, -5.60 , "bypass_urls", 0, 1)) { url-reputation-proxy-redirect(-5.90, -5.60,"",0); }		
3	URL_INAPPROPRIATE	URL_INAPPROPRIATE: if (url-category (['Adult', 'Child Abuse Content', 'Extreme', 'Hate Speech', 'Illegal Activities', 'Illegal Downloads', 'Illegal Drugs', 'Pornography', 'Filter Avoidance'], "bypass_urls", 1, 1)) { duplicate-quarantine("INAPPROPRIATE_CONTENT"); }		
4	DKIM_FAILURE	DKIM_FAILURE: if (dkim-authentication == "hardfail") { duplicate-quarantine("DKIM_FAIL"); }		
5	SPF_HARDFAIL	SPF_HARDFAIL: if (spf-status == "fail") { duplicate-quarantine("SPF_HARDFAIL"); }		
6	EXECUTIVE_SPOOF	EXECUTIVE_SPOOF: if (forged-email-detection("Executive_FED", 90, "")) AND (header("X-IronPort-SenderGroup") != "(?i)allowspoof") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); duplicate-quarantine("FORGED_EMAIL"); }		
7	DOMAIN_SPOOF	DOMAIN_SPOOF: if (header("X-Spoof")) { duplicate-quarantine("ANTI_SPOOF"); }		
8	SDR	SDR: if (sdr-reputation (['awful'], "")) OR (sdr-age ("days", <, 5, "")) { duplicate-quarantine("SDR_DATA"); }		
9	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-RATELIMIT")) { log-entry("X-TG-RATELIMIT: $filenames"); }		
10	BLOCKLIST_QUARANTINE	BLOCKLIST_QUARANTINE: if (true) { quarantine("BLOCKLIST"); }		
11	SAMPLE_ATTACHMENT_BLOCK	SAMPLE_ATTACHMENT_BLOCK: if (attachment-filetype == "Executable") OR (attachment-filename == "\\.(386|ad|ade|adp|asp|bas|bat|chm|cmd|com|cpl|crt|exe|hlp|hta|inf|ins|isp|js|jse|lnk|mdb|mde|msc|msi|msp|mst|pcd|pif|reg|scr|sct|shb|shs|url|vb|vbe|vbs|vss|vst|vsw|ws|wsc|wsf|wsh)$") { duplicate-quarantine("BLOCK_ATTACHMENTS"); drop(); }		
12	SAMPLE_SPF_SOFTFAIL	SAMPLE_SPF_SOFTFAIL: if (spf-status == "softfail") { duplicate-quarantine("SPF_SOFTFAIL"); }		
13	SAMPLE_MACRO	SAMPLE_MACRO: if (macro-detection-rule (['Adobe Portable Document Format', 'Microsoft Office Files', 'OLE File types'])) { quarantine("MACRO"); }		
14	SAMPLE_ATTACHMENT_PROTECTED	SAMPLE_ATTACHMENT_PROTECTED: if (attachment-protected) { log-entry("Encrypted: $MID"); }		
15	SAMPLE_LANGUAGE_UNKNOWN	SAMPLE_LANGUAGE_UNKNOWN: if (message-language == "unknown") { edit-header-text("Subject", "(.*)", "[SUSPICIOUS]\\1"); }		
16	SAMPLE_INAPPROPRIATE_CONTENT	SAMPLE_INAPPROPRIATE_CONTENT: if (dictionary-match("Profanity", 1)) OR (dictionary-match("Sexual_Content", 1)) { quarantine("INAPPROPRIATE_CONTENT"); }		
17	SAMPLE_REPLY-TO_MISMATCH	SAMPLE_REPLY-TO_MISMATCH: if (header("reply-to")) AND (header("reply-to") != "^$envelopefrom$") { add-heading("SAMPLE_REPLY-TO_WARN"); log-entry("REPLY-TO MISMATCH"); }		
18	SAMPLE_EXTERNAL_SENDER	SAMPLE_EXTERNAL_SENDER: if (subject != "[EXTERNAL]") { edit-header-text("Subject", "(.*)", "[EXTERNAL]\\1"); }		
19	SAMPLE_COUNTRY_FILTER	SAMPLE_COUNTRY_FILTER: if (geolocation-rule (['Canada'])) { log-entry("From Canada"); }		

Edit Filter Order...

Filtros de contenido saliente

TG_OUTBOUND_MALICIOUS

Condición: Otro encabezado; encabezado("X-TG-OUTBOUND") == MALWARE

Acción: Cuarentena; cuarentena("TG_OUTBOUND_MALWARE")

Encabezado_secreto_de_banda

Condición: Otro encabezado; encabezado("PLACEHOLDER") == PLACEHOLDER

Acción: Strip Header; strip-header("X-IronPort-Tenant")

EXTERNAL_SENDER_REMOVE

Condición: (Ninguno)

Acción: Agregar/editar encabezado; edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", "")

ACCOUNT_TAKEOVER

Condición: Otro encabezado; encabezado ("X-AMP-Result") == (?i)malintencionado

Condición: Reputación de URL; reputación de URL(-10.00, -6.00 , "", 1, 1)

*Establecer **regla de aplicación: Si una o más condiciones coinciden**

Acción: Notificar;notificar ("<Insertar dirección de correo electrónico de administrador o de distribución>", "POSIBLE ADQUISICIÓN DE CUENTA", "", "ACCOUNT_TAKEOVER_WARNING")

Acción: duplicate-quarantine("ACCOUNT_TAKEOVER")


Filters

Add Filter...

Order	Filter Name	Description | Rules | Policies	Duplicate	Delete
1	Stop_O365_OpenRelay	Stop_O365_OpenRelay: if (header("X-IronPort-Tenant") != "placeholder") { duplicate-quarantine("OPEN_RELAY"); }		
2	TG_OUTBOUND_MALICIOUS	TG_OUTBOUND_MALICIOUS: if (header("X-TG-OUTBOUND") == "MALWARE") { quarantine("TG_OUTBOUND_MALWARE"); }		
3	Strip_Secret_Header	Strip_Secret_Header: if (header("PLACEHOLDER") == "PLACEHOLDER") { strip-header("X-IronPort-Tenant"); }		
4	EXTERNAL_SENDER_REMOVE	EXTERNAL_SENDER_REMOVE: if (true) { edit-header-text("Subject", "\\[EXTERNAL\\]\\s?", ""); }		
5	ACCOUNT_TAKEOVER	ACCOUNT_TAKEOVER: if (header("X-AMP-Result") == "(?i)malicious") OR (url-reputation(-10.00, -6.00 , "", 1, 1)) { notify ("myit@mycompany.com", "POSSIBLE ACCOUNT TAKEOVER", "", "ACCOUNT_TAKEOVER_WARNING"); duplicate-quarantine("ACCOUNT_TAKEOVER"); }		
6	ENCRYPT_OUT	ENCRYPT_OUT: if (subject == "(?i)*encrypt*") { edit-header-text("Subject", "(?i)*encrypt*\\s?", ""); encrypt-deferred ("CRES_HIGH", "$Subject", 0); }		
7	TG_RATE_LIMIT	TG_RATE_LIMIT: if (header("X-TG-OUTBOUND-RATELIMIT")) { tag-message ("NOOP"); }		

Edit Filter Order...

En el caso de los clientes de Cisco Secure Email Cloud, disponemos de filtros de contenido de ejemplo incluidos en la configuración Gold y las recomendaciones de prácticas recomendadas. Además, revise los filtros "SAMPLE_" para obtener más información sobre las condiciones y acciones asociadas que pueden ser beneficiosas para su configuración.

Cisco Live

Cisco Live aloja muchas sesiones a nivel global y no ofrece sesiones presenciales ni sesiones

técnicas que traten las prácticas recomendadas de Cisco Secure Email. Para ver las sesiones y el acceso anteriores, visite Cisco Live (se requiere inicio de sesión de CCO):

- Cisco Email Security: Prácticas recomendadas y ajuste preciso - BRKSEC-2131
- Acelere el perímetro de su correo electrónico - BRKSEC-2131
- Corregir correo electrónico - Resolución de problemas avanzada de Cisco Email Security: BRKSEC-3265
- Integraciones de API para Cisco Email Security: DEVNET-2326
- Protección de los servicios de buzones de correo SaaS con Cloud Email Security de Cisco - BRKSEC-1025
- Seguridad del correo electrónico: Prácticas recomendadas y ajuste preciso - TECSEC-2345
- 250 no OK - A la defensiva con Cisco Email Security - TECSEC-2345
- Protección de dominio de Cisco y protección frente a suplantación de identidad avanzada de Cisco: Saque el máximo partido del siguiente nivel en seguridad para el correo electrónico - BRKSEC-1243
- SPF no es un acrónimo de "simulación". Aprovechemos al máximo la siguiente capa de seguridad para el correo electrónico - DGTL-BRKSEC-2327

Additional Information

Documentación de Cisco Secure Email Gateway

- Release Notes
- Guía del usuario
- Guía de referencia de CLI
- Guías de programación de API para Cisco Secure Email Gateway
- Código abierto utilizado en Cisco Secure Email Gateway
- Guía de instalación del appliance virtual de seguridad de contenido de Cisco(incluye vESA)

Documentación de Secure Email Cloud Gateway

- Release Notes
- Guía del usuario

Documentación de Cisco Secure Email and Web Manager

- Notas de la versión y matriz de compatibilidad
- Guía del usuario
- Guías de programación de API para Cisco Secure Email y Web Manager
- Guía de instalación del appliance virtual de seguridad de contenido de Cisco(incluye vSMA)

Documentación del producto Cisco Secure

- Arquitectura de nomenclatura de la cartera Cisco Secure

Información Relacionada

- Cumplimiento de Cisco Secure Email Security
- Descripción de la oferta: Correo electrónico seguro
- Términos de Cisco Universal Cloud
- Soporte y descargas de Cisco
- [EXTERNO] OpenSPF: Información básica y avanzada de SPF

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).