Universidad de Buenos Aires
Facultades de Ciencias Económicas,
Cs. Exactas y Naturales e Ingeniería

Maestría en
Seguridad Informática

Tesis de Maestría

Aseguramiento del Gateway de correo electrónico

Autor: Claudio Corbellini
Director: Julio Ardita

Año
2024

Cohorte del Cursante
2013

Declaración Jurada de origen de los contenidos

"Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual".

Nombre: Claudio Corbellini

DNI: 30340911

FIRMADO

Resumen

Palabras clave: email, gateway, reputación, spoofing, phishing, anti-malware, anti-virus, filtrado, spam.

Tabla de contenidos

Nómina de abreviaturas

- AMP: Protección avanzada contra software malicioso ("Advance Malware Protection")
- BEC: Ataque de compromiso a los correos electrónicos corporativos ("Business Email Compromise")
- CES: Seguridad de correo en la nube. Solución de seguridad integrada para correo electrónica propietaria de Cisco Inc. ("Cloud Email Security")
- DKIM: Identificación de correos por claves de dominio ("DomainKeys Identified Mail")
- DMARC: Autenticación, reportes y conformidad de mensajes basados en dominio ("Domain-based Message Authentication, Reporting and Conformance")
- IPS/IDS: Sistema de prevención o detección de intrusiones. ("Intrusion Prevention System")
- MTA: Componente de transferencia de correo ("Mail Transfer Agent")
- MX: Servidor de intercambio de correos ("Mail Exchanger")
- PKI: Infraestructura de clave pública ("Public Key Infrastructure")
- RUA: Reporte agregado de resultado de análisis de seguridad emitidos por dominios receptores en un entorno DMARC. ("Report type Aggregate")
- RUF: Reporte forense de resultado de análisis de seguridad emitidos por dominios receptores en un entorno DMARC. ("Report type Forensic")
- SBRS: Base de datos de reputación de emisores de correo electrónico ("Sender Base Reputation Score")
- SaaS: Software como servicio ("Software as a service")
- SEG: Gateway de seguridad de correo electrónico ("Secure Email Gateway")
- SPF: Marco de convenio entre remitentes ("Sender Policy Framework")

- SMTP: Protocolo para transferencia simple de correo (“Simple Mail Transfer Protocol”)
- SSL: Seguridad de la capa de transporte (“Secure Sockets Layer”)

Cuerpo introductorio

La confianza en el envío, recepción y confidencialidad del correo electrónico resulta hoy en día un aspecto de seguridad crítico en la infraestructura de comunicaciones de cualquier organización.

Los ataques de tipo Business Email Compromise (BEC) y Spoofing, han tenido un crecimiento exponencial en los últimos años. Colocándolos entre los ataques con mayores pérdidas reportadas anualmente por el Centro de Crimen en Internet (IC3 - Internet Crime Complaint Center) del FBI de Estados Unidos [1].

By Complaint Loss			
Crime Type	*Loss*	*Crime Type*	*Loss*
Investment	$4,570,275,683	Extortion	$74,821,835
BEC	$2,946,830,270	Employment	$70,234,079
Tech Support	$924,512,658	Ransomware*	$59,641,384
Personal Data Breach	$744,219,879	SIM Swap	$48,798,103
Confidence/Romance	$652,544,805	Overpayment	$27,955,195
Data Breach	$534,397,222	Botnet	$22,422,708
Government Impersonation	$394,050,518	Phishing/Spoofing	$18,728,550
Non-payment/Non-Delivery	$309,648,416	Threats of Violence	$13,531,178
Other	$240,053,059	Harassment/Stalking	$9,677,332
Credit Card/Check Fraud	$173,627,614	IPR/Copyright and Counterfeit	$7,555,329
Real Estate	$145,243,348	Crimes Against Children	$2,031,485
Advanced Fee	$134,516,577	Malware	$1,213,317
Identity Theft	$126,203,809		
Lottery/Sweepstakes/Inheritance	$94,502,836		

Reporte anual del FBI IC3 2024 - perdidas confirmadas por tipo de ataque durante el año 2023 [1].

Durante muchos años el correo electrónico se mantuvo como un sistema simple y eficiente, que no requería de sistemas especiales dedicados avanzados para su funcionamiento.

Pero a medida que fueron creciendo las necesidades de elevar sustancialmente el nivel de seguridad de las comunicaciones por correo, apareció una nueva solución en el ámbito de la infraestructura tecnológica de las organizaciones: el Gateway de correo electrónico, también conocido como SEG (Security Email Gateway)

Actualmente los Gateway de correo electrónico más sofisticados se alojan en infraestructuras distribuidas en la nube, brindando una enorme cantidad de funciones y posibilidades para mejorar la seguridad en las comunicaciones, muchas de estas nuevas funcionalidades a veces son desconocidas por los responsables en Ciberseguridad.

No suele darse un buen uso a toda la potencialidad en seguridad de la que disponen. Esto se debe a varios factores, entre los que se incluyen: la relativa novedad de estas funcionalidades, la falta de conocimiento en el mercado por ser un nicho tan específico, el hecho que usualmente los administradores de estas soluciones no suelen ser expertos en seguridad, y a dificultades técnicas inherentes propias de un sistema complejo.

El objetivo de este trabajo es primero hacer una descripción general de cómo funciona un Gateway de correo electrónico (SEG) de última generación dentro de una infraestructura híbrida típica actual.

Se analizarán los proveedores y las productos más conocidos, y cómo se posiciones actualmente en cuanto a liderazgo. Para poder profundizar en las características y configuraciones específicas se hará foco en la solución Cisco CES ("Cloud Email Security"), que es una de las soluciones líderes del mercado.

Se analizará en detalle las etapas en la que cada correo electrónico debe pasar dentro del sistema. Cómo operan internamente cada módulo, y que impacto tienen en seguridad. Se verá cómo efectuar adecuadamente las configuraciones recomendadas para una correcta implementación de SPF, DKIM y DMARC.

El objetivo es proponer configuraciones, reglas y el diseño de funciones de seguridad específicas que se pueden implementar en un Gateway de correo electrónico corporativo para aumentar el nivel de protección contra BEC ("Business Email Compromise")/Spoofing, Phishing y Spam, entre otros, para reducir de forma significativa la exposición a este tipo de ataques.

Finalmente se verán las últimas tendencias recientes en cuanto a la de evolución de analíticas avanzadas e Inteligencia Artificial (AI), para la detección temprana de ataques en correos basados en análisis de contenido e interpretación de lenguaje natural.

Este trabajo continúa y complementa los aspectos de seguridad esenciales y ataques más conocidos al correo electrónico que fueron encarados en el Trabajo final de especialización en Seguridad Informática "Ataques y protección en el servicio de correo electrónico".[2]

Cuerpo Principal

1 La aparición del Gateway de correo electrónico

A principios de los años 2000, el volumen de tráfico correo electrónico tuvo un crecimiento exponencial, acompañado por la expansión de Internet. En esto años el Spam resultaba ser tan voluminoso que generaba no solo incomodidad para los usuarios, sino una sobrecarga de los sistemas procesamiento de correo que dedicaban la mayor parte de su tiempo a distribuir este contenido no deseado.

Si bien varias compañías comenzaron a brindar soluciones a este problema, tal vez la más emblemática fue una empresa originaria de San Bruno, California, llamada IronPort Systems Inc [3].

Ironport fue una de la primeras compañías en comercializar Gateways de correos electrónico dedicados, con funcionalidades enfocadas en seguridad. Estas soluciones luego fueron también llamadas SEG (Gateway de seguridad de correo electrónico - "Security Email Gateway")

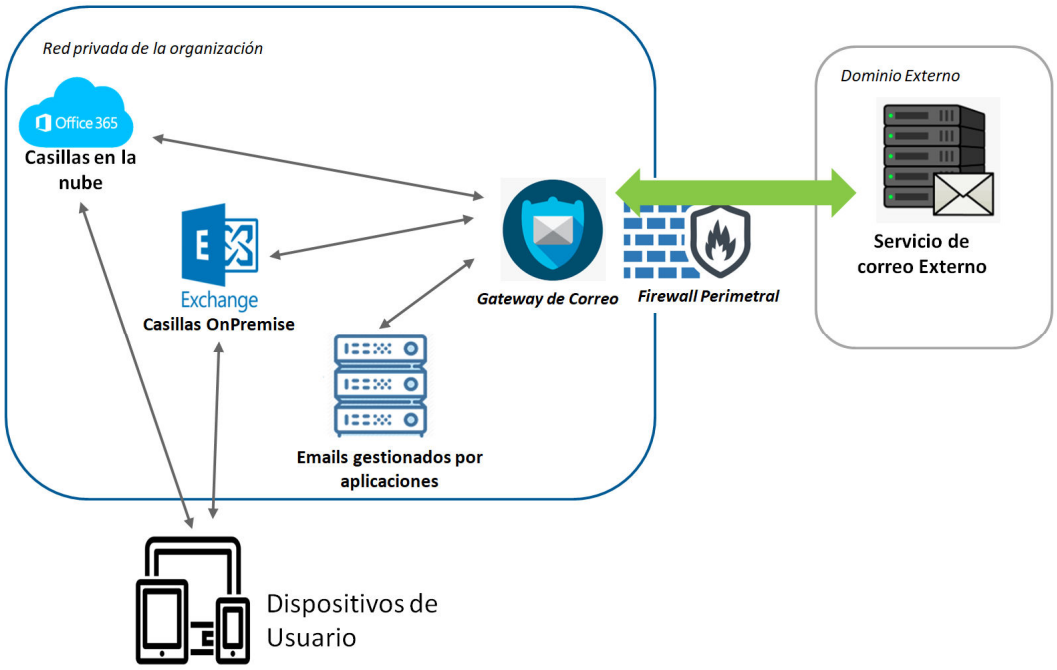
Se trataban de equipos físicos dedicados ("hardware appliance"), que integraban principalmente funciones AntiSpam que funcionaba junto a un sistema de reputación de dominios central llamado "SenderBase". Este servicio descubría y calificaba con una puntación a todos los dominios de Internet que eran emisores de correo electrónico.

En el año 2007 la empresa fue adquirida por Cisco Systems [3], que continuó con todos los productos y que fue la base para su propia expansión en las soluciones de Gateway de correo electrónico.

Si bien los nuevos sistemas han evolucionado mucho desde entonces, el diseño de la arquitectura central de la solución de Ironport se mantiene aún vigente en la soluciones SEG/CES de Cisco.

2 Ubicación en la infraestructura

El Gateway de correo electrónico actúa como perímetro del ingreso y egreso de mensajes. Es el encargado de administrar las conexiones con los servidores de correo de origen/destino, y actuar como proxy con los servicios de correo que la organización utilice.



Ubicación conceptual del Gateway de correo en una arquitectura Híbrida

El Gateway de correo generalmente se ubica detrás del firewall perimetral, y siempre adelante de todos los servicios de correo (OnPremise

y/o Cloud), manejando todas las conexiones SMTP entrantes y salientes de la organización.

Llamamos una arquitectura híbrida de correo, a aquella en la que la organización utiliza servicios de correo electrónico en Cloud (Por ejemplo Exchange Online de Microsoft, o Gmail de Google), pero en la que además se mantienen servidores de correos OnPremise en el centro de datos propio.

Este es el modelo más habitual que encontramos en organizaciones que comenzaron migrar de forma paulatina a la nube, y mantienen ambas infraestructura durante el proceso. Pero también lo vemos en grandes empresas que deciden mantenerlo de forma permanente por temas de rendimiento, confidencialidad o costo de licenciamiento.

3 Funciones principales del Gateway de correo

El Gateway de correo (o SEG) está diseñado no sólo para cumplir funciones de seguridad, sino que de forma primordial es el componente básico que ahora maneja cada conexión con servidores de correo externo, el enrutamiento de cada correo. Es decir que cumple las funciones de lo antes se separaba conceptualmente en Componente de transferencia de correo (MTA o "Mail Transfer Agent") y Servidor de intercambio de correos (MX o "Mail Exchanger").

Una solución de Gateway de correo puede atender de forma simultánea múltiples dominios distintos, cada uno con diferentes configuraciones y destinos independientes.

Pero su aspecto más relevante hoy en día son sus funciones de seguridad. Entre las funciones que las soluciones más avanzadas generalmente disponen, se pueden destacar:

- Antispam
- Antivirus
- Clasificación y filtrado de dominios emisores

- Servicios de cifrado y protección de correo electrónico
- Integración con Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
- Sandboxing y protección avanzada contra malware
- Desarmado y reconstrucción de contenido (CDR - "Content Disarm and Reconstruction")
- Prevención de fuga de datos ("DLP")
- Des-suscripción segura de listas de envío ("Safe-Unsubscribe")
- Filtrado de brotes infecciosos ("Outbreaks Filters")
- Protección posterior a la entrega ("Post-Delivery Protection")

Si bien algunos proveedores tienen diferentes nombres comerciales para estas protecciones, las funciones suelen ser básicamente las mismas, a las que ahora se están comenzando a sumar características avanzadas de análisis de contenido, pero aún se encuentran en etapas muy tempranas de desarrollo. A éstas nuevas funcionalidades, casi experimentales, les dedicaremos un apartado más adelante.

4 Soluciones en el mercado

Hoy en día nos encontramos con una gran cantidad de proveedores que ofrecen este tipo de soluciones de Gateway de correo electrónico.

Para tener un panorama de compañías y productos, nos remitimos al el relevamiento publicado en "Software Reviews" durante este año 2024 sobre las soluciones disponibles durante el año 2023, elaborado por el grupo de investigación "Info Tech Research Group" [4].

Productos y proveedores líderes durante el año 2023:

- Abnormal Security (Abnormal Security)
- Armorblox (Armorblox)
- Avanan (Check Point Software Technologies Ltd.)

- Barracuda Email Security Gateway (Barracuda Networks)
- Cisco Secure Email (Cisco Systems)
- Cloud App Security (Trend Micro)
- IRONSCALES (IronScales Ltd)
- Microsoft Exchange Online Protection (Microsoft Corporation)
- Mimecast Email Security & Resilience (Mimecast Services)
- Perception Point (Perception Point Ltd)
- Proofpoint Advanced Threat Protection (Proofpoint)
- SpamTitan (TitanHq)
- Vade Secure for Microsoft 365 (Vade Secure)

Otros productos más pequeños con funciones de seguridad de correo electrónico similares a un SEG, pero en general más limitados a determinados escenarios específicos:

- Acronis Cyber Protect Cloud Email Security (Acronis)
- Barracuda Essentials (Barracuda Networks)
- Barracuda Sentinel (Barracuda Networks)
- Cellopoint (Cellopoint International Corp.)
- Censornet Email Security (Censornet)
- Clearedin (Clearedin)
- Clearswift Secure Email Gateway (Fortra)
- CYREN Email Security (CYREN)
- Darktrace/Email (Darktrace)
- Forcepoint DLP for Email (Forcepoint LLC)
- FortiMail (Fortinet)
- Fortra Agari Phishing Defense (Fortra)
- GreatHorn Cloud Email Security (GreatHorn Inc)
- Hornet Security (Hornetsecurity)
- INKY (Inky Technology)
- InterScan Messaging Security (Trend Micro)
- Proofpoint Essentials Email Security (Proofpoint)
- Retarus Email Security (Retarus)

- Sealit (Sealit Technologies Ltd.)
- Sonicwall Email Security (SonicWall)
- Symantec Email Security.cloud (Broadcom Inc.)
- Symantec Messaging Gateway (Broadcom Inc.)
- Trellix Email Security (Trellix)
- Trustwave Secure Email Gateway (Trustwave)
- Vircom modusCloud (Vircom Inc)
- WithSecure Elements Collaboration Protection (WithSecure)

La solución de Microsoft (Exchange Online Protection) que comenzó más bien relegada frente a los jugadores que tenían más años en el mercado, está teniendo un muy rápido crecimiento debido a las mejoras que están incorporando al producto y a la cantidad de usuarios potenciales que tiene al añadir las funcionalidades de forma nativa a su plataforma, con lo que suma rápidamente clientes que ya vienen utilizando productos de Office365.

Como vemos, existe una gran variedad de tipo de productos, algunos se comercializan como equipos físicos de hardware (tipo "appliances"), otros sólo son licencias de software a ser instalados en equipos propios. Pero la tendencia actual es cada vez más productos que se venden como servicios en la nube (cloud SaaS), en la cual los usuarios no necesitan saber cómo los proveedores implementan técnicamente la solución en sus centros de datos.

5 El análisis de dominios y las bases de reputación

La mayoría de las soluciones de Gateway de correo trabajan de una u otra forma con alguna base de datos en la que categorizan todos los dominios de Internet que emiten correos.

Estas enormes bases son similares a las que utilizan los sistemas de Proxy para Internet, en la que se necesitan clasificar todos los sitios web para poder luego aplicar filtros de contenido para la navegación segura. Esta

tarea titánica tiene una gran parte automatizada, pero que también requiere cierta intervención humana para poder catalogar más específicamente cada sitio, generalmente usando redes colaborativas.

En el caso de las bases de dominios emisores de correo electrónico el objetivo es más puntual, se logra utilizando casi exclusivamente datos generados de forma automática y derivados de la clasificación del dominio ya realizado para las funciones web. El objetivo final es poder determinar un puntaje de reputación del dominio en base a su actividad histórica. Estas bases de datos de reputación de dominios emisores suelen llamarse SBRS ("Sender Base Reputation Score")

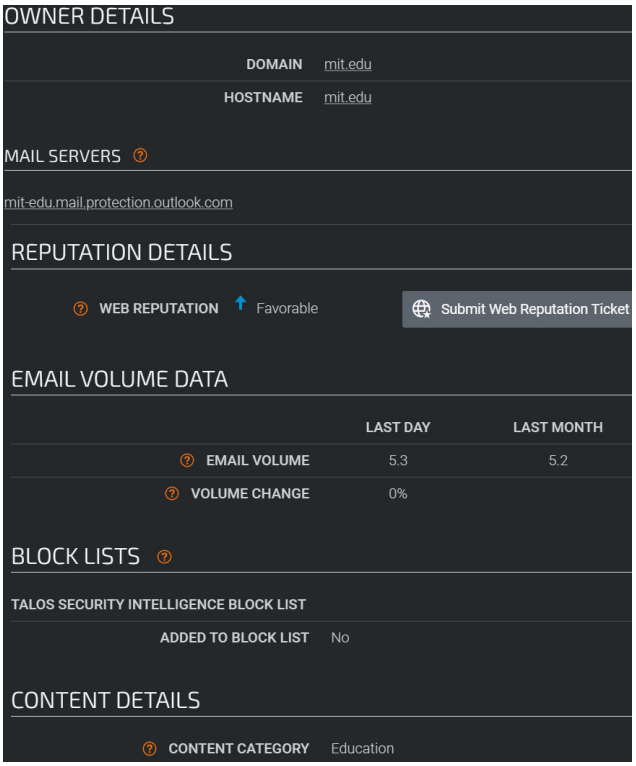
Por ejemplo en el caso de Cisco, la empresa mantiene un sistema de inteligencia sobre amenazas integrado llamado "Talos" [5]. En el mismo se concentran varias tipo de datos y amenazas diversas, entre las que se destacan:

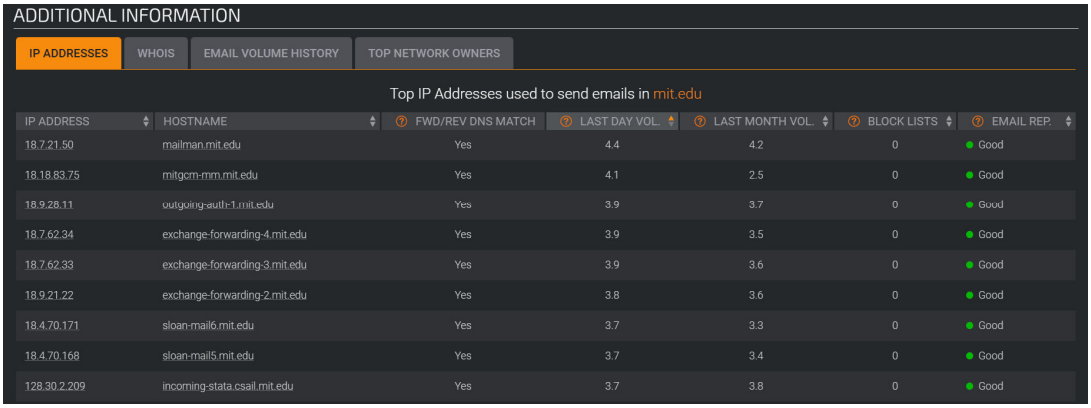
- Reputación Web (puntaje de cada sitio Web, mayormente usado para funciones de Proxy y sistemas Anti-Phishing)
- Categorización de contenido (la clasificación de cada sitio Web, mayormente usado para funciones de Proxy)
- Reputación por Dominio Emisor (específicamente para correo electrónico)
- Reputación por IP emisora (similar al anterior, pero por direccionamiento específico independiente del dominio)
- Reputación de archivo (estas son firmas para identificar archivos maliciosos conocidos, similar a lo que manejaría un sistema Antivirus)
- Bases de CVE ("Common Vulnerabilities and Exposures") (Mayormente usados para funciones de tipo IPS/IDS)

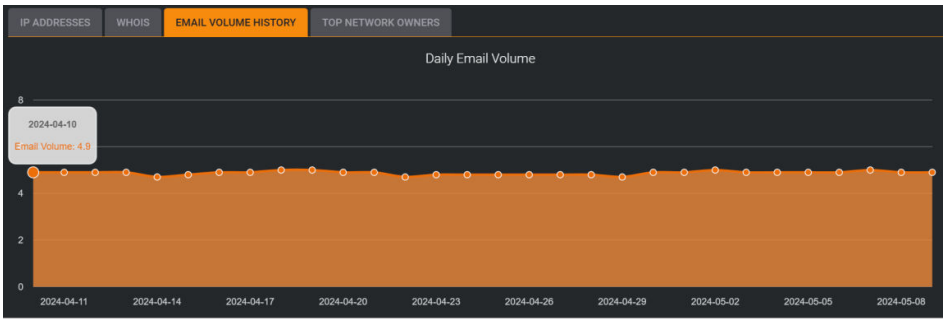
En el caso de Cisco SBRS, las puntuaciones de reputación de emisores de correos pueden oscilar entre -10 y +10, lo que refleja la probabilidad de que una dirección esté intentando enviar contenido no deseado. Las puntuaciones muy negativas indican que es muy probable que

los remitentes envíen spam. Cuando se acercan a 0, son neutrales, o sea que en general tienen poca o mixta reputación. Cuando son muy positivas tienen buena reputación y son orígenes confiables que pueden ser aceptados sin mayores filtros de contenido.

Ejemplo de la información de un emisor de correo ("mit.edu"), disponible en el sistema Talos de Cisco [6]:







Información de reputación de emisor, actividad por IP y volumen diario de correos relacionadas al dominio "mit.edu", obtenidas del sistema Cisco Talos [6].

Analizando los registros DNS y MX, la historia del dominio, volumen de tráfico de correos, y reportes de lista negras, el sistema determina una puntuación general que puede utilizarse como filtro básico. La información más detallada que la componen se podría usar para filtros más avanzados en casos específicos, por ejemplo para no aceptar correo de un dominio que sea muy nuevo.

6 La arquitectura de un Gateway de seguridad de correo

Para poder avanzar en el estudio técnico y de configuración de un Gateway de correo, necesitamos elegir algunas de las soluciones disponibles para mostrar el detalle de su diseño y funcionamiento.

En este trabajo tomamos como ejemplo representativo del mercado la solución de seguridad de correo de Cisco: Secure Email Gateway/Cloud Email Security (CES).

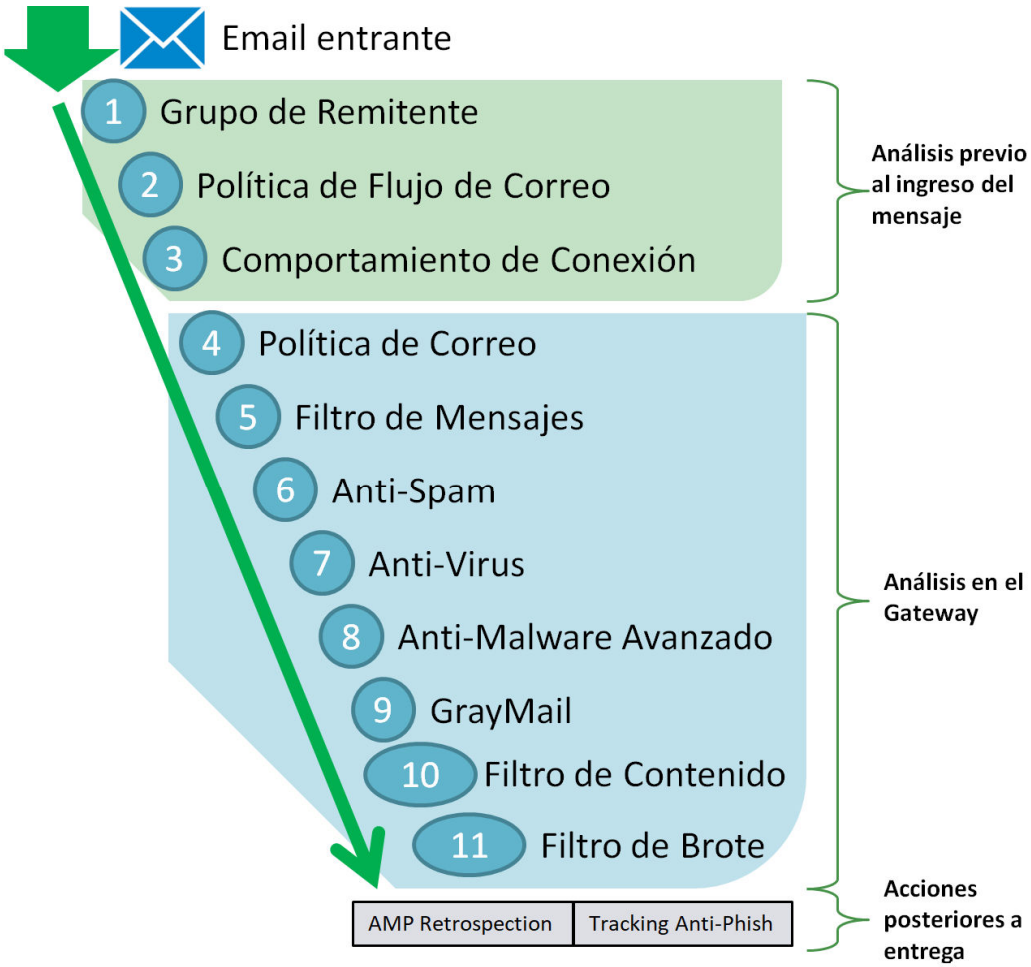
La solución se comercializa como un servicio (SaaS), y está implementado en una nube distribuida, a la cual se deben re direccionar los registros MX de la organización para que apunten al nuevo destino.

Las organizaciones que utilizan un sistema de protección de Cisco se pueden identificar porque sus registros públicos MX apuntan al dominio " iphmx.com".

6.1 Etapas análisis de correos entrantes

En el esquema CES cada mensaje debe transitar por 11 etapas de análisis y filtros hasta ser entregado en el sistema de correo del cliente [7].

En el siguiente gráfico se resumen las etapas, y el orden en que se ejecutan:



Etapas de procesamiento de un mensaje entrante

Estas etapas pueden subdividirse en 3 categorías principales:

- Las que se ejecutan antes de que la transmisión del mensaje se inicie.
- Las actividades de análisis con el contenido del correo antes de entregarse.
- Funciones que pueden realizarse posterior a la entrega del mensaje al servicio de correo.

1. **Grupo Remitente** ("Sender Group")

En esta primera etapa en base al dominio/IP que quieren iniciar una nueva conexión, se consulta su reputación en la base de reputación (SBRS). En base a la puntuación y características relevadas, se le asigna un Grupo Remitente. Este grupo lo clasifica en alguna de las categorías definidas previamente y determinará los flujos posteriores a los que será sometido el mensaje.

Los grupos pueden ser definidos por:

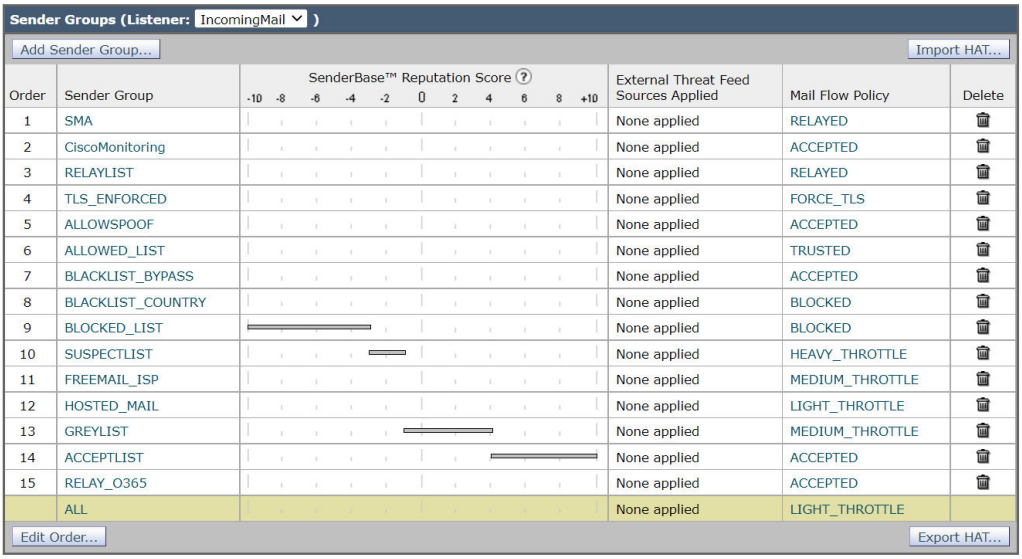
- Dirección o rango IP
- Host específico o nombre de dominio
- Lista DNS
- Clasificación de IP Reputation Service
- Puntuación de reputación de IP Reputation (IPRS)

Se dispone de los siguientes grupos de remitentes generales pre-definidos por defecto:

Grupo remitente	Descripción	Política de Flujo de Correo
ALLOWED_LIST	Se agregan a esta lista los remitentes en los que se confía. La política de flujo aplicada es $TRUSTED. Según CISCO esta se encuentra configurada para que	TRUSTED

Grupo remitente	Descripción	Política de Flujo de Correo
	no tenga habilitada la limitación de velocidad y que el módulo Anti-Spam no analice el contenido de dichos mensajes.	
ACCEPTLIST	Remitentes con calificación muy alta, que pueden transitar con controles muy ágiles y cuya prioridad es garantizar las entregas sin trabas ni demoras.	ACCEPTED
BLOCKED_LIST	Los remitentes de dicho grupo son rechazados, generalmente con puntuación de reputación muy negativa. Agregar remitentes manualmente a este grupo directamente rechaza las conexiones de esos hosts.	BLOCKED
SUSPECTLIST	En este grupo se encuentran aquellos remitentes que se consideran sospechosos. La política de flujo aplicada define que se realicen análisis muy rigurosos por todos los módulos de seguridad.	HEAVY_THROTTLED
GREYLIST	Remitentes con puntuación baja, pero no negativa. Muy posible que hagan envío de correos por suscripción y algo de Spam. Se les aplica una política media, para pasar todos los controles de seguridad con controles balanceados.	MEDIUM_THROTTLE
RELAYLIST	Remitentes definidos manualmente que se sabe deberían poder retransmitir al grupo definido internamente como seguro.	RELAYED
ALL	Es el grupo de remitentes que aplica para todos aquellos que no hayan ingresado en ninguno de los parámetros anteriormente definidos.	ACCEPTED

Para entender cómo se aplican los grupos según la escala general de reputación se muestra como se ven desde la consola de configuración:



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	CiscoMonitoring		None applied	ACCEPTED	
3	RELAYLIST		None applied	RELAYED	
4	TLS_ENFORCED		None applied	FORCE_TLS	
5	ALLOWSPOOF		None applied	ACCEPTED	
6	ALLOWED_LIST		None applied	TRUSTED	
7	BLACKLIST_BYPASS		None applied	ACCEPTED	
8	BLACKLIST_COUNTRY		None applied	BLOCKED	
9	BLOCKED_LIST		None applied	BLOCKED	
10	SUSPECTLIST		None applied	HEAVY_THROTTLE	
11	FREEMAIL_ISP		None applied	MEDIUM_THROTTLE	
12	HOSTED_MAIL		None applied	LIGHT_THROTTLE	
13	GREYLIST		None applied	MEDIUM_THROTTLE	
14	ACCEPTLIST		None applied	ACCEPTED	
15	RELAY_O365		None applied	ACCEPTED	
	ALL		None applied	LIGHT_THROTTLE	

Edit Order... | Export HAT...

Definición de grupo de remitentes, clasificación según escala de puntuación indicado en rangos y política que le aplicará a cada uno

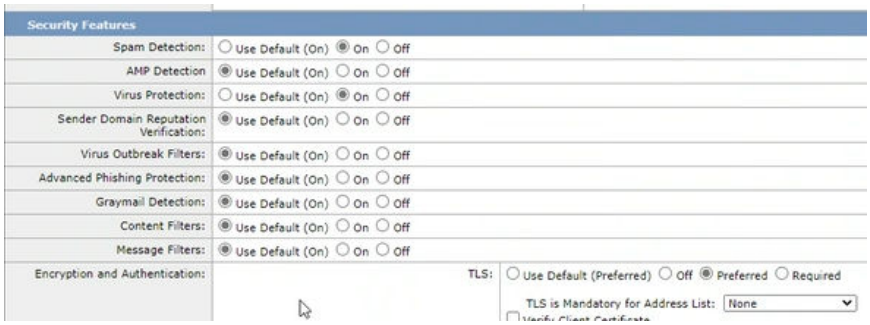
Todos los grupos se pueden definir con miembros (dominios o IP) de forma manual, pero para los demás casos no indicados específicamente a mano, los grupos de definirán en base a su puntuación de reputación.

Podemos ver en el gráfico de ejemplo que los grupos con puntuación muy negativa se envían directamente a BLOCKED_LIST, los de puntuación no tan negativa a SUSPECTLIST, los de puntuación baja a GREYLIST, y los de muy alta puntuación a ACCEPTLIST.

2. **Política de Flujo de Correo** ("Mail Flow Policy")

En base al grupo remitente en el que fue clasificado, aquí se determina que pasos y módulos deberá transitar obligatoriamente. Por ejemplo si el mensaje deberá pasar por el módulo Anti-Spam, GrayMail, etc. Ya que, por ejemplo, un correo de un dominio muy confiable, no necesitará siquiera pasar por estos módulos.

La lógica es que el mensaje sólo se hará pasar por los módulos/herramientas que son necesarios según su origen.



Ejemplo selección de módulos a aplicar a una Poítica de Flujo de Correo

3. **Comportamiento de Conexión** ("Connection Behavior")

En esta etapa se define si se permitirá al emisor realizar el envío del contenido del mensaje vía SMTP. Hasta esta instancia el emisor sólo se ha identificado con el Gateway solicitando iniciar el envío de un correo. Pero es en esta etapa que, en base a los controles reputacionales previos, se aprueba que continúe o no con la transmisión.

Esta fase es crítica, ya que permite bloquear de forma muy temprana muchos tipos de ataques de denegación de servicio, así como también a emisores que sólo generan Spam y cuyas voluminosas transmisiones del contenido afectarían innecesariamente la performance de la infraestructura.

La acción de cortar la conexión en esta instancia no tiene casi costo de procesamiento para el Gateway y significa que podrá rechazar de forma masiva múltiples intentos de ataques simultáneos.

4. **Política de Correo** ("Mail Policy")

Así como durante la segunda etapa se definía que módulos se debían transitar, aquí se define el detalle de cómo se aplicará la configuración de cada módulo/herramienta para cada mensaje. Por ejemplo que umbral se aplicará para definir si es Spam, acciones a realizar si se

encuentra Malware, que hacer si se encuentran links a páginas web en dominios externos, etc.

5. **Filtro de Mensajes** ("Message Filter")

Son filtros y acciones básicas que se pueden realizar mayormente a nivel de datos de encabezado del mensaje. Se pueden establecer reglas para, por ejemplo, enviarlo a una cuarentena si la dirección del remitente no coincide con el dominio desde el que se recibió el mensaje. O si se encontrara alguna otra inconsistencia a nivel del encabezado.

En esta etapa se pueden también agregar meta datos al encabezado para identificar alguna característica que lo destaca. Se puede por ejemplo modificar un asunto para agregar alguna advertencia al usuario final, por ejemplo que se trata de un email desde un dominio externo sospechoso (con poca reputación conocida).

6. **Anti-Spam**

Controles y acciones a ejecutar si el mensaje tiene signos de ser posible Spam. Ya sea: ser descartado, ser enviado a cuarentena, etc.

El módulo calcula un puntaje ponderado a varias variables que incluye, reputación de dominio de origen, dirección de origen y de retorno, cantidad de destinatarios, entre otras. Con esto se determina la puntuación numérica con la que luego se configura cuál rango considerar como positivo de Spam y cual como sospechoso.

En general a las cuarentenas de Spam no se les hace una revisión manual, y se descartan luego de unos 30 o 60 días. Pero sirven para recuperar algún mensaje puntual que se identifique o se reclame por algún usuario, en caso de que fuera un falto positivo.

7. **Anti-Virus**

Se envía cada mensaje a un motor de Antivirus, y se definen las acciones en caso que se detecte contenido peligroso. Por ejemplo se

determina que si se encuentra un adjunto con virus, si debería ser reparado, o eliminado, o si el mensaje completo debe ser enviado a cuarentena. Si se agrega un texto en el mail indicando que se encontró un adjunto con virus. Cómo proceder si un archivo adjunto parece ser contenido cifrado que no se puede analizar, etc.

8. **Anti-Malware Avanzado** ("Advance Malware Protection - AMP")

Este módulo adicional al Anti-Virus permite detectar amenazas específicas que no suelen ser encontradas con un reconocimiento de firmas estático tradicional. Haciendo uso de técnicas de Sandboxing, se detectan comportamiento de Malware que se identifican recién al abrir los archivos. Ejemplos clásicos son archivos de Microsoft Office o Adobe Acrobat (PDF), que tienen Scripts o contenido interactivo que puede resultar malicioso.

9. **GrayMail**

El objetivo es la identificación de correos que son generalmente de información, noticias, promociones, notificaciones, u otros correos que los usuarios de forma legítima se subscribieron en algún momento. Pero ya sea por el volumen excesivo, desinterés u otros motivos, ya han perdido relevancia y no tienen utilidad real. Una vez identificados se puede definir acciones como descartar, enviar a un carpeta específica, etc.

10. **Filtro de Contenido** ("Content Filter")

En esta etapa se inspecciona el contenido completo del correo, y se permite crear todo tipo de reglas para identificar elementos o patrones y tomar acciones personalizadas. No hay limite a la complejidad de reglas que pueden crearse. Utilizando un lenguaje de programación propio se permite el uso de funciones, variables y diccionarios (constantes). Más adelante profundizaremos sobre cómo podemos mejorar la seguridad del correo creando reglas propias desde este módulo.

11. **Filtro de Brote** ("Outbreak Filter")

En esta último módulo permite identificar y detener, mientras se están produciendo, ataques que son desconocidos por los motores de Antivirus, pero que se logran identifican por características reportadas a nivel global por diferentes clientes y análisis de tráfico realizados por Cisco, desde diversas fuentes. O sea son ataques masivos a nivel global que tienen patrones reconocibles por la forma que se expanden y el volumen, y que si bien aún no se tiene el detalle exacto de cómo ocurren, se pueden detener preventivamente en base a características comunes hallados en las direcciones de origen, encabezados, adjuntos, contenido, etc.

Post entrega

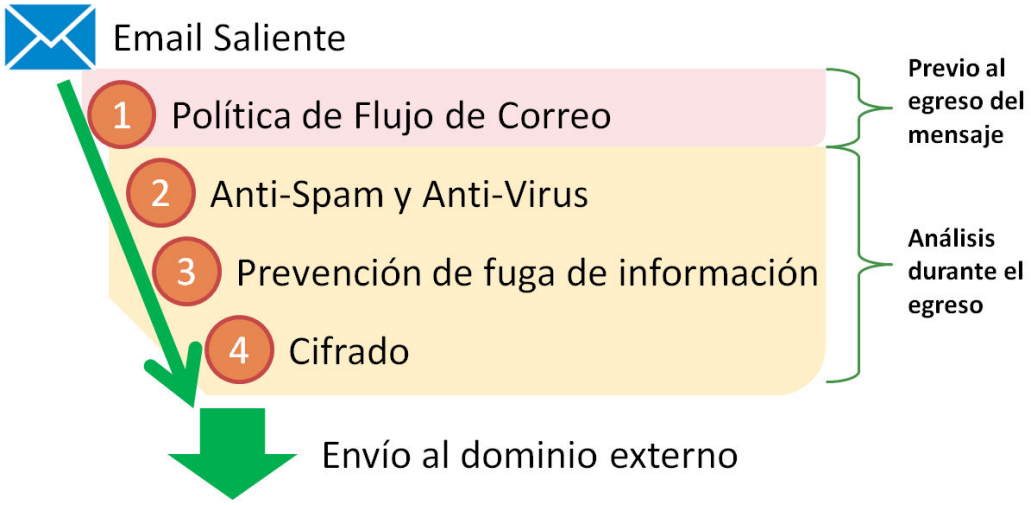
Luego de estas 11 etapas el correo se entrega al sistema destino, pero se continúan monitoreando 2 procesos posteriores a esto. Que son el "AMP Retrospection" y el "Tracking Anti-Phish"

En el primero, relacionado al sistema avanzado contra malware, se identifican y registran los archivos que parecían posiblemente sospechosos cuando pasaron por el módulo, pero que no había evidencia suficiente como para detenerlos en ese momento. Para hacer un seguimiento de todos los correos que contienen estos elementos y poder hacer tareas de depuración posteriores en caso que se confirme como ataques a estos destinatarios [8].

Por último el sistema de "Tracking Anti-Phish", se refiere a que generalmente los links sospechosos identificados en el contenido de los mail se los modifica para re direccionarlos para que pasen por un portal seguro, en vez de ir directamente al link externo en Internet. Entonces desde este portal se va haciendo seguimiento de los usuarios que hicieron clic en los links, y en caso de confirmar que se trata de páginas de Phishing, se los puede bloquear, además de obtener un reporte de los usuarios que cayeron en el engaño.

6.2 Etapas análisis de correos salientes

El esquema que se aplica a correos salientes es obviamente mucho más corto y simple que para los entrantes. Consta de un máximo de 4 etapas, según la configuración y políticas definidas [7].



Etapas de procesamiento posibles de un mensaje saliente [7]

1. **Política de Flujo de Correo** ("Mail Flow Policy")

Igual que con el flujo de ingreso, se pueden indicar que según un grupo remitente definido previamente, se determine qué pasos y módulos deberá transitar obligatoriamente durante la salida. Por ejemplo se podría optar por hacer controles Anti-Spam sólo a los mail originados desde aplicaciones o sistemas, y obviar estos controles adicionales para correos originados desde casillas de usuarios finales.

2. **Anti-Spam y Antivirus**

La lógica de los controles en esta instancia de salida, tiene que ver con la protección de usuarios e infraestructura así como el cuidado de la reputación del propio dominio.

El módulo antivirus podría funcionar como una capa adicional de seguridad a los controles del Antivirus local de cada estación de trabajo, o para capturar contenido originado desde terminales no seguras (por ejemplo dispositivos móviles obsoletos sin soporte de seguridad).

Las funciones Anti-Spam podrían usarse para evitar que usuarios internos hagan uso indebido de la infraestructura con fines personales. Así como prevenir por ejemplo los casos en que malas configuraciones, de aplicaciones o servidores, inundan el tráfico con mail generados automáticamente de forma incorrecta. Si estos correos salieran a Internet afectarían el puntaje de reputación del dominio propio.

3. **Prevención de fuga de información** ("DLP")

En este módulo se pueden agregar diferentes tipo de controles para evitar que información clasificada sea fugada vía correo electrónico. Se realiza un análisis completo de contenido y adjuntos para buscar patrones previamente definidos por la organización como posibles indicios de fugas. El ejemplo clásico son por ejemplo los patrones de número de tarjetas de crédito, o números de identificación personal como los de seguridad social en Estados Unidos. Generalmente los correos sospechosos se envían a una cuarentena para ser inspeccionados manualmente por personal de algún área de seguridad de la información o riesgos.

4. **Cifrado**

Esta módulo optativo se trata en este caso de una solución específica de Cisco ("Secure Email Encryption"), en la que se brinda un mecanismo para cifrar contenido en un correo en un formato HTML, con un sistema de almacenamiento de claves en la nube.

Soluciones a medida similares para el envío de correos electrónico cifrado nunca han tenido éxito en el mercado. Ya que se encuentran con serias limitaciones de compatibilidad y de usabilidad. En este caso puntal para utilizarlo se requiere luego acceder de forma autenticada a una web

para obtener la clave o instalar un Add-in compatible para clientes Outlook para Windows para poder visualizar el correo.

Estas técnicas de intentar cifrar el contenido de correos con mecanismos externos a los estándares de correo electrónico, no parece que tuvieran futuro en el ámbito de la seguridad. Tal vez para un uso muy limitado entre un grupo de organizaciones puntuales.

Con una implementación adecuada de conexiones cifradas para la transmisión de los mensajes (usando SMTPS), y con la correcta implementación de SPF, DKIM y DMARC, tanto por el emisor como por el receptor, el cifrado de contenido pierde relevancia y generalmente no sería necesario. [2]

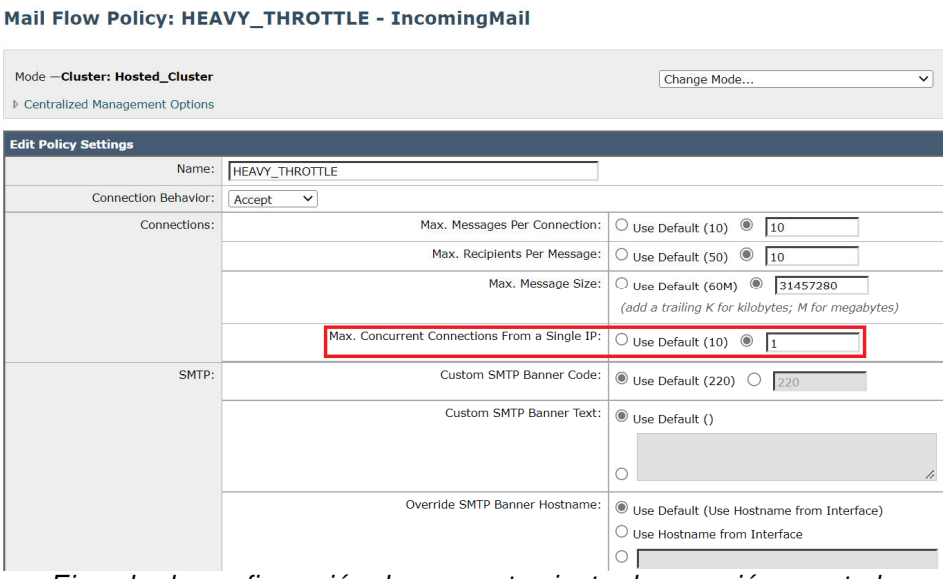
7 Mejoras en la seguridad general

Ahora que vimos muy resumidamente la arquitectura y etapas generales para el procesamiento de mensajes, avanzaremos con las mejoras que se puedan implementar a las configuraciones y circuitos estándares para lograr un nivel de seguridad mayor a lo que se obtiene por defecto en soluciones de Gateway de correo.

7.1 Optimizar el manejo de conexiones

Como vimos un punto clave para evitar los ataques de denegación de servicio y detener todo tipo de ataques de forma muy temprana es el manejos de conexiones aceptadas.

Para aumentar la seguridad, se podría definir un flujo más exigente para las conexiones con origen de baja reputación, estableciendo un límite de mensajes, destinatarios por conexión y tamaño total. Y no permitiendo conexiones concurrentes desde la misma IP (parámetro "Max. Concurrent Connections From a Single IP"):



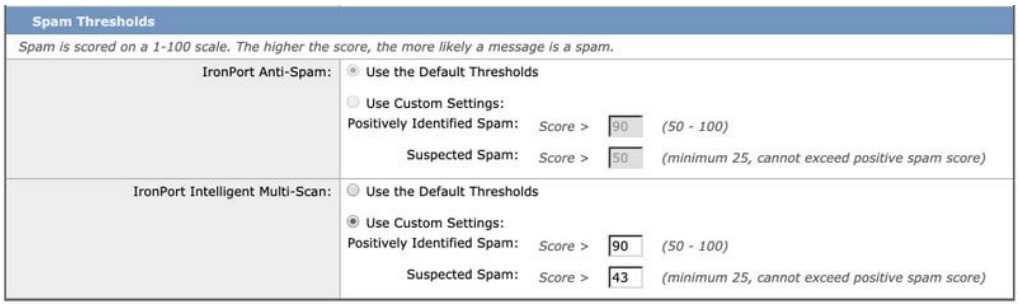
Ejemplo de configuración de comportamiento de conexión aceptados para un circuito más exigente al normal

Esta recomendación no sólo evita ataques clásicos con mucha cantidad de conexiones y volumen, sino que también hace que los dominios de alta reputación tengan prioridad para el uso de conexiones y mayor velocidad. Al obligar a los dominios de baja reputación a esperar la transmisión de forma limitada usando 1 conexión a la vez, y un menor número de mensajes totales por cada una.

7.2 Mejoras en los filtros de Spam

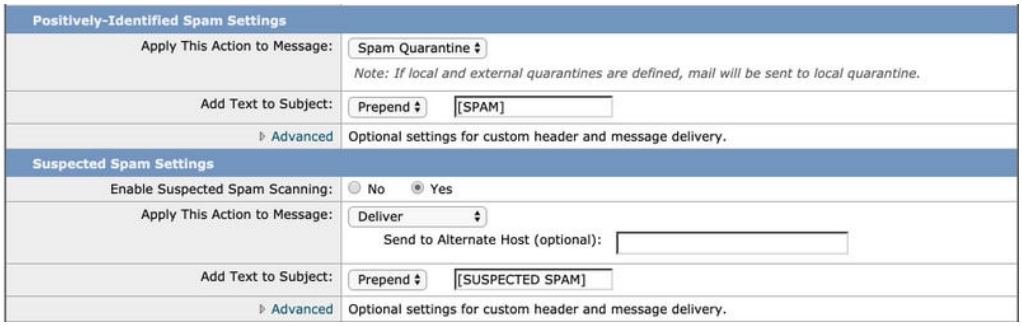
A fin de reducir al mínimo el Spam, pero evitando perder mensajes de posible interés, se recomienda hacer un mejor uso de las puntuaciones calculadas para separar en dos tipo de mensajes de Spam: los positivos y los sospechosos.

Para el caso de Cisco CES la mejor combinación es haciendo uso del "Ironport Intelligent Multi-Scan", definir un rango mayor de 90 para clasificarlos como positivos de Spam, y un valor desde 43 (un valor que surge de pruebas y algunas recomendaciones del propio proveedor) para identificarlos como sospechoso [9].



Selección de rangos para considerar un mensaje como Spam positivo y como sospechoso

Con esta clasificación conviene modificar los asuntos de los correos para claramente identificarlos como Spam o sólo como posible Spam. Con el objetivo de separar los positivos enviándolos directamente a una cuarentena manual, pero los sospechoso entregarlos al usuario para que él decida si son o no de utilidad. El usuario podría, si lo desea, aplicar filtros propios en su cliente de correo para enviar estos mail ya identificados a alguna carpeta propia para revisión.



En el ejemplo se envía a cuarentena los mensajes de Spam y se entregan con una advertencia al usuario los mensajes sospechosos.

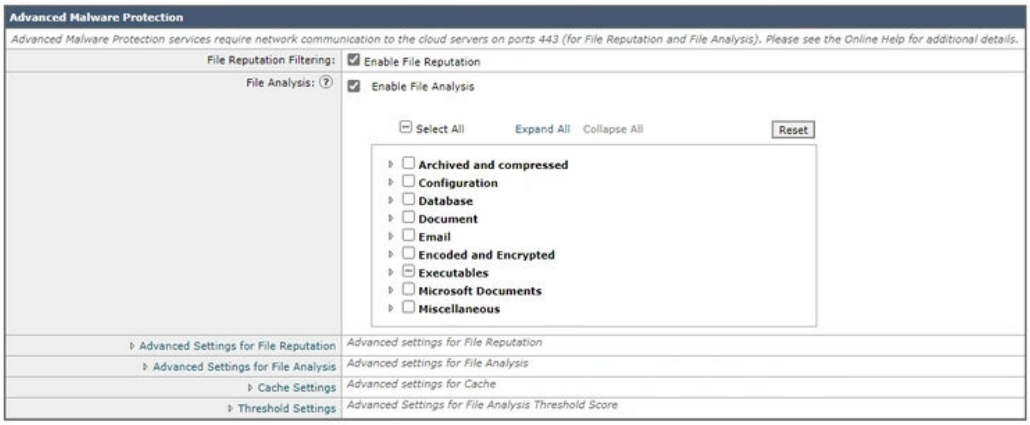
En caso de identificar un falso positivo, y recuperarse manualmente algún mail enviado como positivo a cuarentena, también le llegarían al usuario ya identificado con la leyenda Spam en el asunto para que sepa el motivo por el que había sido retenido.

7.3 Recomendaciones en protección Anti-Malware

Hay que entender que el Anti-Malware Avanzado (AMP) tiene 3 tapas de funciones separadas.

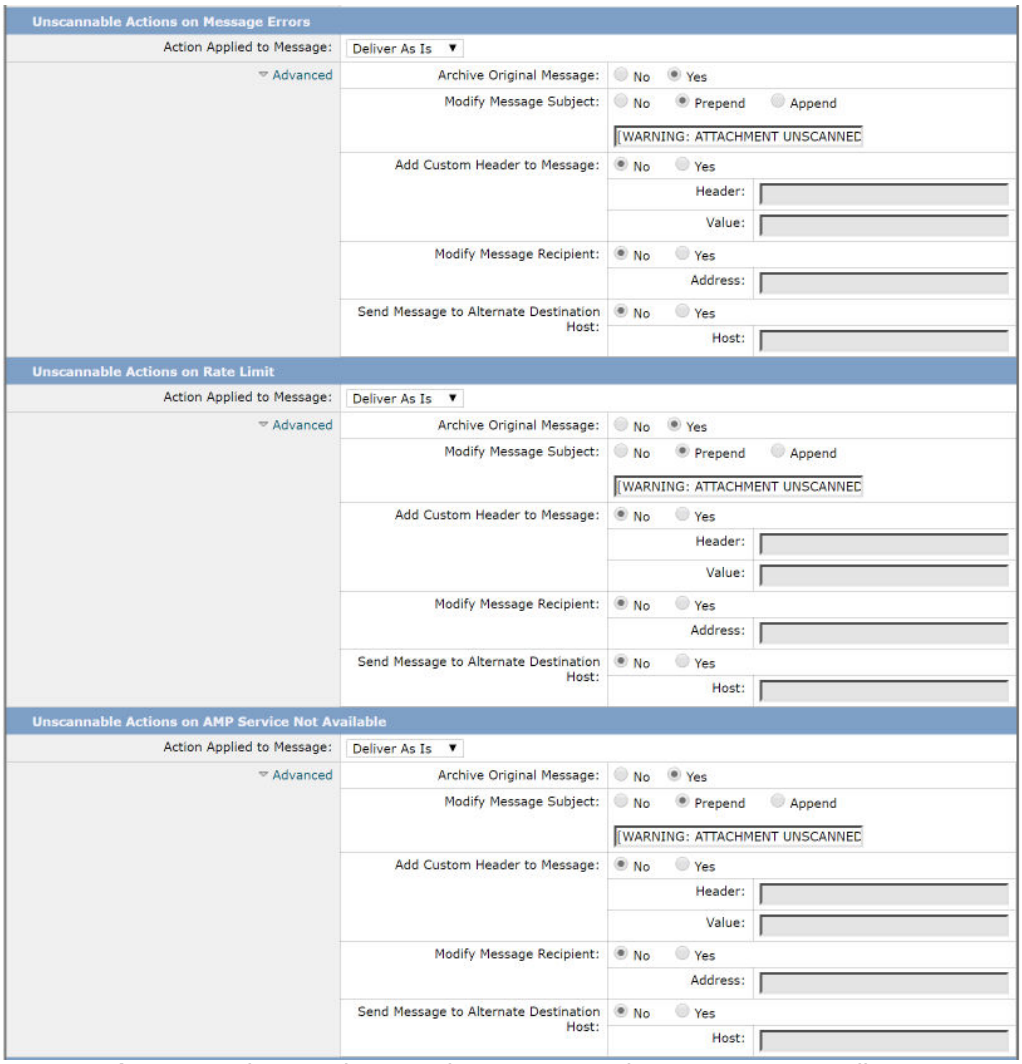
- Reputación de archivos: se calcula un Hash de cada archivo (para identificarlo de forma única) y se lo envía a la red de inteligencia basada en la nube para una evaluación de reputación. Esto es para identificar archivos previamente reportados como peligrosos. Obviamente el archivo infectado se analiza como un conjunto, por lo que no debe tener cambios (mutaciones).
- Análisis de archivos en tiempo real: Usando técnicas de Sandboxing se define el comportamiento del archivo durante su apertura/ejecución para determinar el nivel de amenaza del adjunto.
- Remediación automática de casillas ("Mailbox Auto Remediation" - MAR): permite eliminar correos electrónicos con archivos que se identificaron como maliciosos posterior a su entrega en cada casilla. Esto es útil para reducir el riesgo de ataques muy recientes, que se están identificando mientras están en progreso.

Lo que debe prestar atención es que las 3 funciones estén activas y apliquen a todos los tipo de archivos que se van sumando al soporte. No es común que generen falsos positivos, así que mejor utilizarlos para todos los tipos soportados.



Módulos AMP activos, y selección de tipos de archivos a los que aplica

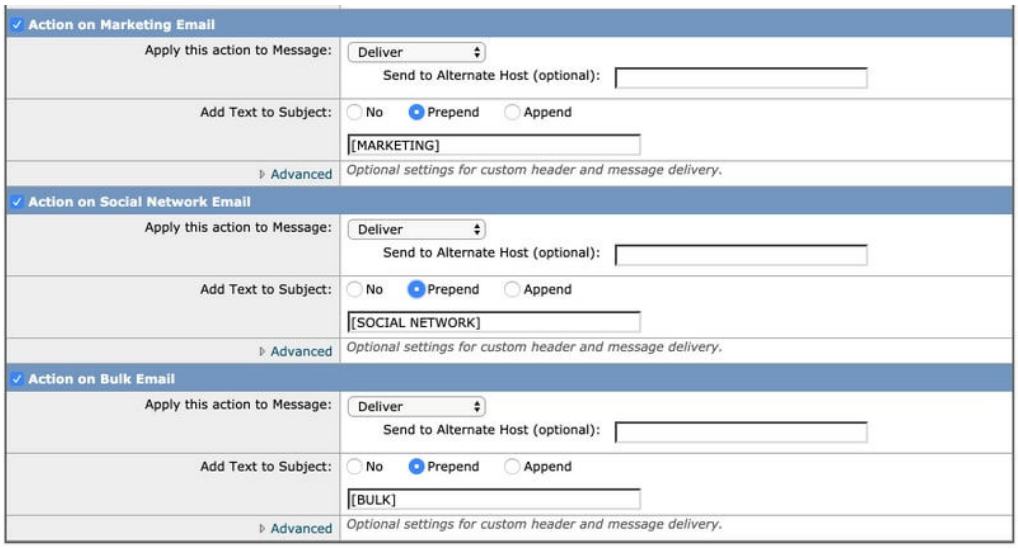
Otra recomendación es identificar con mensajes para los usuarios todos los archivos que no han podido ser escaneados por los módulos de protección. Si bien también se podría optar por directamente detener los adjuntos que no se pudieron procesar, esto genera un gran problema para las organizaciones en las se usan archivos cifrados por los usuarios, generalmente en contenedores comprimidos .zip. Por lo que es mejor priorizar la disponibilidad y dejarlos transitar, pero con advertencias [10].



Agregar advertencias en el asunto para los correos con adjuntos que no pudieron ser analizados por estar cifrados u otros motivos técnicos [10]

7.4 Clasificación de GrayMail

Una buena práctica que se puede aplicar al correo con material promocional, publicitario, de divulgación, conocido como "GrayMail" es también pre clasificar el contenido para el usuario. Los sistemas de reputación definen en base a varios patrones que tipo de contenido tienen, por lo que resulta muy útil hacer que esta información llegue al usuario final vía un texto que los etiquete en el Asunto del correo [9].



Reenvío de clasificación automática al usuario vía modificación de Asunto en cada correo.

Con esta función el usuario tiene clasificado el contenido en: Marketing, Redes Sociales, correo masivo, etc. Y se le delega a cada uno la posibilidad, por ejemplo, de enviarlos a carpetas personales agregando filtros a nivel de cliente de correo, si así lo deseara.

8 Técnicas específicas contra el Spoofing/BEC

Las buenas prácticas anteriores, suman seguridad general para varias amenazas, pero en mi opinión la función más importante que debe realizar el Gateway de correo es prevenir lo mejor posible los ataques de Spoofing, que generalmente son usados como parte de un ataque combinado de compromiso de correos corporativos (BEC).

La base fundamental para la prevención del Spoofing, siguiendo la de cumplir con los protocolos publicados por la Internet Engineering Task Force's (IETF), que son: la correcta implementación del Marco de convenio entre remitentes (“Sender Policy Framework” o SPF) y de la Identificación de correos por claves de dominio (“DomainKeys Identified Mail” o DKIM), para llegar finalmente una política segura con la Autenticación de Mensajes

Basada en Dominios, Informes y Conformidad (Domain-based Message Authentication, Reporting and Conformance, o "DMARC") [2].

Una vez que se esté cumpliendo con DMARC, recomendaría empezar a aplicar técnicas más avanzadas del análisis de encabezado y contenido con el objetivo de identificar correos sospechosos por sus patrones específicos. Entre las técnicas que se describirán se hará un gran uso del módulo y reglas de "Filtro de Contenido" mencionado anteriormente entre las etapas de análisis de correos entrantes.

8.1 La importancia de SPF, DKIM y DMARC

El Gateway de correo electrónico cumple un rol fundamental en el cumplimiento de los protocolos estándares de seguridad. Es desde este equipo en que se centraliza el cumplimento de los protocolos: SPF para asegurar el origen autorizados de las comunicaciones, DKIM para validar cada encabezado vía firma digital y DMARC para el control, monitoreo y aseguramiento de todo el circuito de comunicaciones de correo electrónico.

El detalle de funcionamiento de estos 3 protocolos están descriptos en el trabajo final de Especialización: "Ataques y protección en el servicio de correo electrónico"[2]. Repasando muy brevemente los conceptos generales:

SPF permite al dueño de un dominio de Internet publicar cuales direcciones IP están autorizadas para enviar un correo electrónico a su nombre, utilizando los ya existentes registros del Sistema de nombres de dominio (DNS) en un registro MX (Mail Exchanger record).

DKIM permite al receptor verificar que un correo electrónico que afirma originarse en un dominio haya sido autorizado por el dueño de ese dominio al sumar una firma digital a cada correo saliente. El sistema destinatario lo verifica buscando la clave pública del remitente. Con un control de integridad, la firma garantiza que el encabezado del correo electrónico tiene el origen que indica y no haya sido modificado. Las firmas DKIM no son visibles para los usuarios finales, sólo sirven a los efectos de la

verificación que se realiza internamente en la infraestructura de correo electrónico.

DMARC tiene 2 funciones básicas, por un lado tiene que ver con la publicación por parte de cada dominio de su política de seguridad en cuanto a los correos que emite, y la segunda función está asociada a la publicación de direcciones para un sistema automático de notificaciones para controlar que los receptores están recibiendo los correos correctamente, sin fallas en los controles de seguridad y alertar de posibles intentos de spoofing.

Con DMARC una nueva entrada en el registro DNS/MX se agrega a las anteriores. El dominio emisor debe definir y publicar en qué estado se encuentra básicamente en cuanto a su nivel de implementación de SFP y DKIM. Cada administrador de dominio de correo debe elegir entre 3 políticas posibles que reflejan el estado actual en cuanto a su nivel de seguridad de correo electrónico:

- "None" (Ninguno): es la política de nivel de entrada. Los receptores saben que el emisor no es seguro por lo que no deben rechazar los emails sin seguridad, pero permite que un dominio reciba informes de monitoreo de las recepciones.
- "Quarantine" (Cuarentena): pide a los receptores que traten con sospecha los mensajes que no pasan la verificación de seguridad. Los diferentes receptores tienen diferentes medios para implementar esto, por ejemplo marcar mensajes con algún "tag" o entregarlos , o dejarlos en cuarentena para una revisión manual.
- "Reject (Rechazar): pide a los receptores que rechacen por completo los mensajes que no superen la verificación DMARC (SPF y DKIM). Es la política de mayor seguridad.

Para poder ir monitoreando el avance desde una política insegura "None" hasta llegar a una de alta seguridad "Reject", DMARC ofrece un sistemas de notificaciones para estar al tanto de si los correos están

pasando los controles del tercero correctamente, o si está fallando algunos de los controles SFP o DKIM.

Existe 2 tipos de reportes:

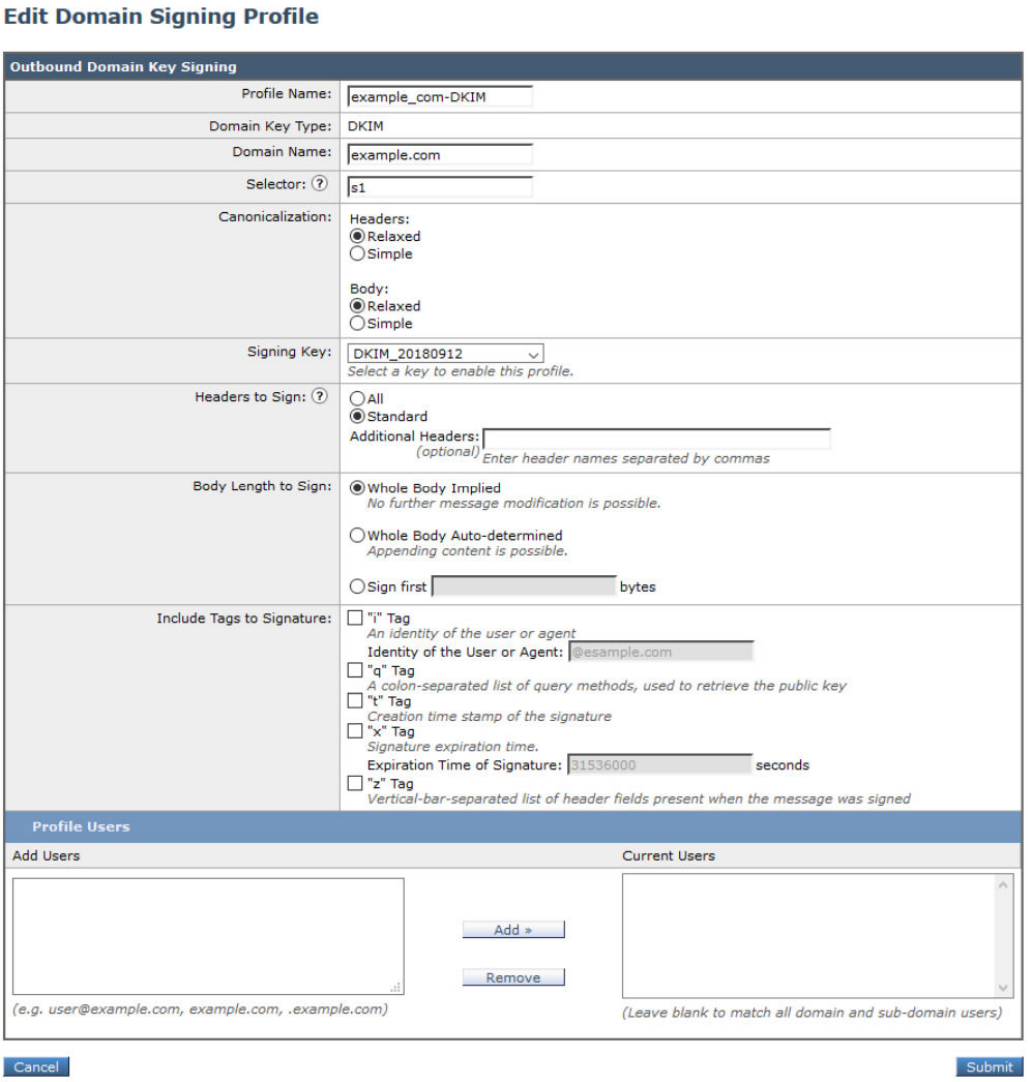
- RUA (reportes agregados o de resumen): se envían como archivos XML, normalmente una vez al día. El asunto menciona el "Dominio del informe", que indica el nombre de dominio DNS sobre el cual se generó el informe.
  Contiene un resumen del total de las recepciones con ese dominio, con el resultado de las verificaciones de seguridad.
- RUF(reporte forense): Los informes forenses, también conocidos como informes de fallas, se generan en tiempo real y consisten en copias de mensajes individuales que fallaron SPF o DKIM. Permiten analizar individualmente cada caso.

8.2 La configuración SPF

El Gateway debería centralizar todas las comunicaciones de correo electrónico de la organización, por lo que sabemos que tenemos un único origen de correos salientes. Lo que se simplifica el registro de SPF a la dirección o nombre DNS definido como dirección publica del mismo, generalmente el nombre o rango asignado por el proveedor de servicio de Gateway de correo en la nube. (para soluciones SaaS)

8.3 La configuración DKIM

Para firmar digitalmente todos los correos salientes, sólo debemos generar o importar la clave privada de nuestra infraestructura PKI, crear un perfil de DKIM y aplicarlo a los correos salientes. Si tenemos varios dominios o selectores, cada uno tendrá un perfil distinto con diferente juegos de clave pública/privada.



Ejemplo configuración de perfil DKIM en Cisco CES

8.4 La matriz DMARC para tráfico entrante

En el Gateway de correo debe configurarse para los flujos entrantes que acciones se van a tomar para la verificación en cada protocolo de seguridad, según cada política publicada por los terceros emisores.

Por defecto se cuentan con 3 perfiles para DMARC (no confundir con la política publicada en el registro DNS/MX):

- Monitoreo ("Monitor"): Se deja ingresar todos los mails independientemente de lo solicitado por el emisor. Es decir que el resultado de los controles SPF y DKIM son ignorados, y no se bloquean los mensajes que fallaron los controles.

- Cuarentena ("Quarentine"): Si el emisor tiene una política "Reject", los mensajes que hayan fallado SPF/DKIM se envía a una cuarentena, sino se dejan pasar.

- Imponer ("Enforce"): Se cumple exactamente la política publicada por el emisor. Si su política fuera "None", los mensajes se dejan pasar sin validaciones. Si fuera "Quarantine", los mensajes que fallaran controles de seguridad se envían a una cuarentena. Si el emisor tuviera una política "Reject", cualquier mensaje que fallara algún control de seguridad sería directamente descartado.

Profile Name	Reject Policy Message Action	Quarantine Policy Message Action	SMTP Action
MONITOR	No Action	No Action	Accept
QUARANTINE	Quarantine	No Action	Accept
ENFORCE	Reject	Quarantine	Accept

Matriz de cumplimiento de política DMARC del emisor en el Gateway

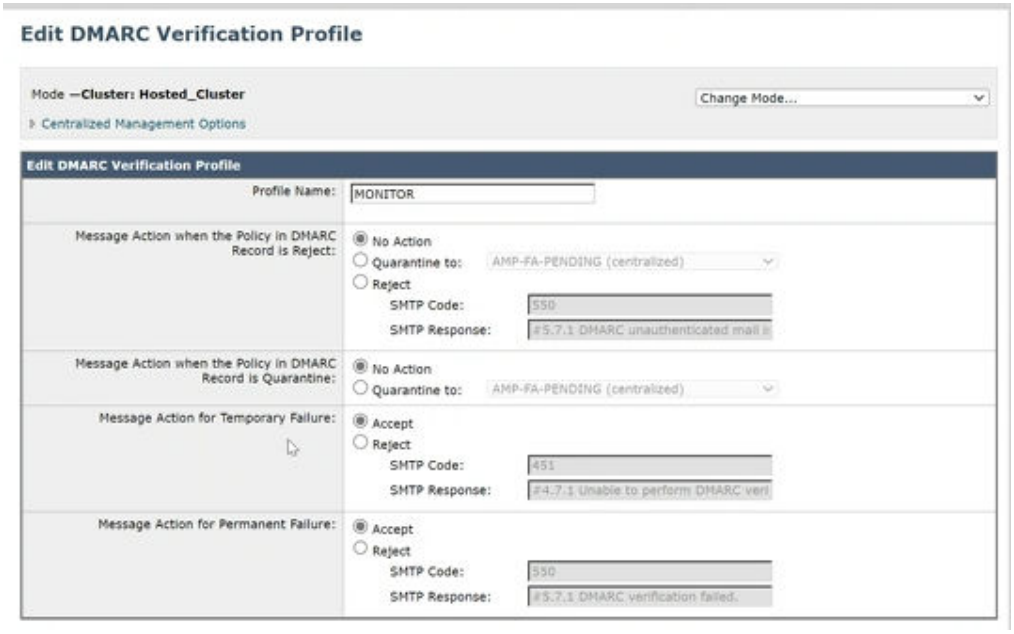
Obviamente para cumplir DMARC como fue diseñado, el receptor debería tener siempre configurado su política de ingreso en "Enforce" para todos sus flujos de ingreso de correos. El hecho de que exista una matriz de reinterpretación de lo que ya define el emisor como un comportamiento seguro para los correos que emite, puede resultar bastante confuso.

Personalmente no veo mucha utilidad de la existencia de esta matriz. En la realidad lo que ocurre es que debido al desconocimiento previo de cómo operan la triada SPF, DKIM y DMARC, los administradores, en la confusión general, eligen una configuración que priorice la alta disponibilidad seleccionado un perfil "Monitor" para los flujos de ingreso.

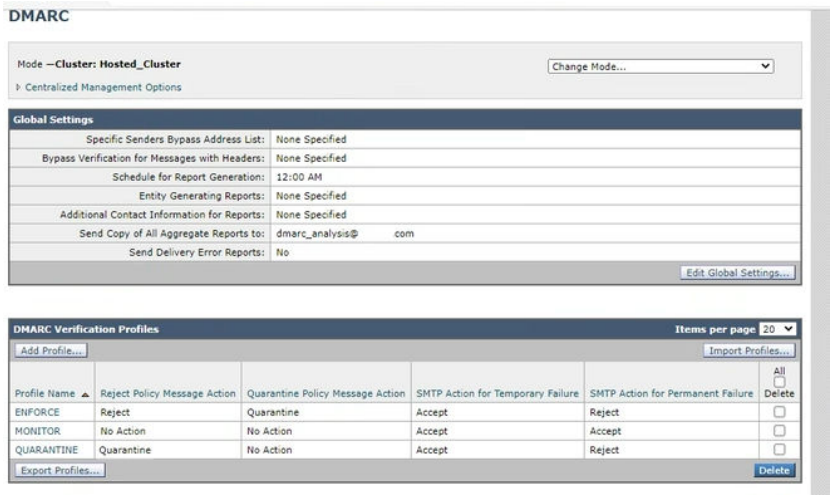
Lo cierto es que los perfiles de monitoreo y cuarentena de esta matriz deberían ser sólo para pruebas en caso que no se tenga confianza del cumplimiento de DMARC por parte de terceros.

Sería muy improbable que un dominio publique una política segura de rechazo ("Reject"), sin antes verificar que está cumpliendo plenamente con todos sus controles de seguridad que garanticen el normal funcionamiento de SPF y DKIM. En todo caso la responsabilidad sería siempre del emisor, que verá los rechazos en los reportes agregados (RUA) de DMARC, y no del receptor que impone correctamente la política publicada.

También por desconocimiento o confusión, algunas organizaciones establecen una política de ingreso "Monitor", específicamente para los dominios de mayor confianza (por ejemplo incluidos en una "Whitelist"). Este es el peor caso, ya que se desperdicia toda la inversión de seguridad realizada por el tercero, al dejar pasar como válidos los mails generados con orígenes no verificados. Y justamente se aplica para las organizaciones conocidas, con la cuáles se debería mantener el nivel de seguridad más elevado posible.



Ejemplo de definición del perfil "Monitor" en Cisco CES



Resumen de perfiles de verificación DMARC en Cisco CES

8.5 Inspección de reportes RUA y RUF

Si bien algunas compañías están comenzado a brindar herramientas para hacer de forma automatizada el análisis de los reportes de RUA y RUF, es una tarea que puede realizarse de forma manual.

Recordemos que en los reportes se reciben como un mail en una casilla definida [2]. Ya que la información está contenida como adjuntos .XML. Una metodología que resulta práctica es descargar todos los archivos en un directorio local para hacer analíticas utilizando un servidor SQL o usando Microsoft PowerBI, por ejemplo.

Debido a que, en una infraestructura madura, la mayoría de los reportes RUA se devuelven sin errores de autenticación, podemos enfocarnos solamente en aquellas entradas que reporten "Fail", ya sea durante el chequeo SPF o el DKIM.

En aquellas entradas que en las que veamos que sólo unos pocos mails fueron rechazados por el receptor por no pasar las verificaciones de seguridad, muy posiblemente estemos viendo intentos fallidos de realizar un ataque de Spoofing.

En este ejemplo vemos un dominio que reporta gran cantidad de correos recibidos con éxito desde nuestra organización "ejemplo.com", pero sospechosamente 1 solo fue rechazado.

org_name	email	report_id	domain	source_ip	count	dkim	spf	selector	result
Citi	dmarc.reports.rua@citi.com	2340031540	ejemplo.com	129.138.32.122	156	pass	pass	ejemplo-onmicrosoft	pass
Citi	dmarc.reports.rua@citi.com	2340031540	ejemplo.com	129.138.32.124	87	pass	pass	cer1	pass
Citi	dmarc.reports.rua@citi.com	2340031540	ejemplo.com	69.141.155.133	1	fail	fail	free_cert	fail

Reporte RUA con 1 solo mail rechazado por el destinatario

Es muy probable que este se tratara de un intento de suplantación de nuestro dominio, y gracias a este análisis basado en el reporte RUA enviado por un tercero ahora tenemos identificada la IP utilizada para suplantar nuestra identidad, para poder continuar con una investigación o directamente para reportarla como fuente de Spoofing.

En caso de que adicionalmente se reciben reportes forenses (RUF), con este podemos completar con un análisis detallado de cada caso identificado previamente con el reporte de resumen RUA. Los reportes RUF son especialmente útiles para investigar los intentos de suplantación por parte de terceros que hacen uso ilegítimo de un dominio que no les pertenece. Su uso forma una red de monitoreo, soportada en forma colaborativa por todos los receptores posibles en Internet, y mantienen al tanto al dueño real del dominio con la información útil para investigar o denunciar servidores, direcciones y dominios, que están intentado hacer Spoofing [2].

En un reporte RUF, entre otros datos, se incluye:

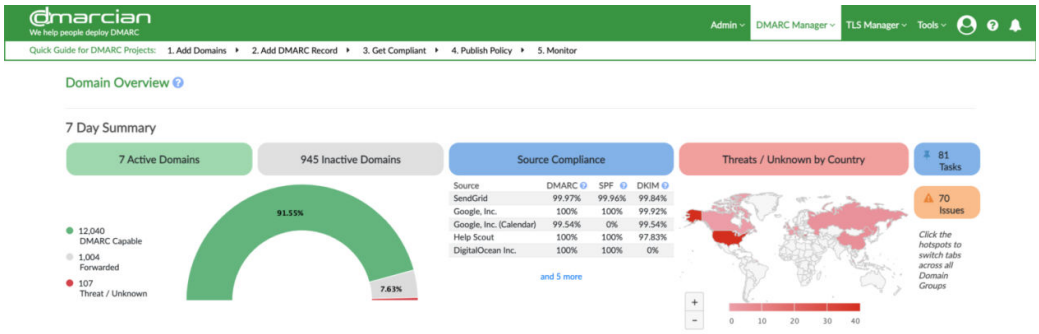
- IP de conexión del envío
- From (dirección de origen que afirma tener)
- To (Destinatarios)
- Asunto del correo electrónico
- Resultados de autenticación SPF y DKIM
- Fecha/hora recibida
- Encabezados de mensajes que incluyen el host de envío, el ID del mensaje de correo electrónico, la firma DKIM.

El análisis en detalle de un reporte forense RUF, es más que suficiente para poder identificar el origen, e incluso las posibles motivaciones u objetivos del ataque de Spoofing. En ocasiones permite también identificar el intento del desvío de comunicaciones hacia dominios "look-alike", que a veces ya figuran en copia del mail del atacante, o que pueden ser obtenidos del encabezado desde el campo de retorno "reply-to".

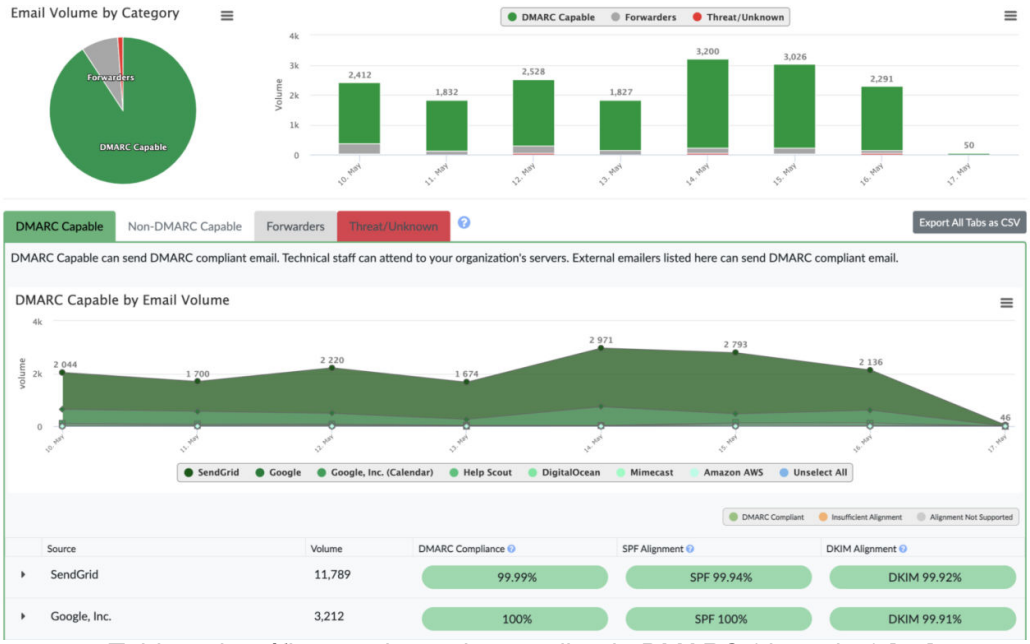
8.5.1 La solución "dmarcian"

En diciembre del 2021, Cisco se asoció con la compañía " dmarcian" especializada en DMARC (de hecho su fundador fue uno de los que desarrollaron el estándar original), para integrar sus servicios con las funcionalidades que provee [11].

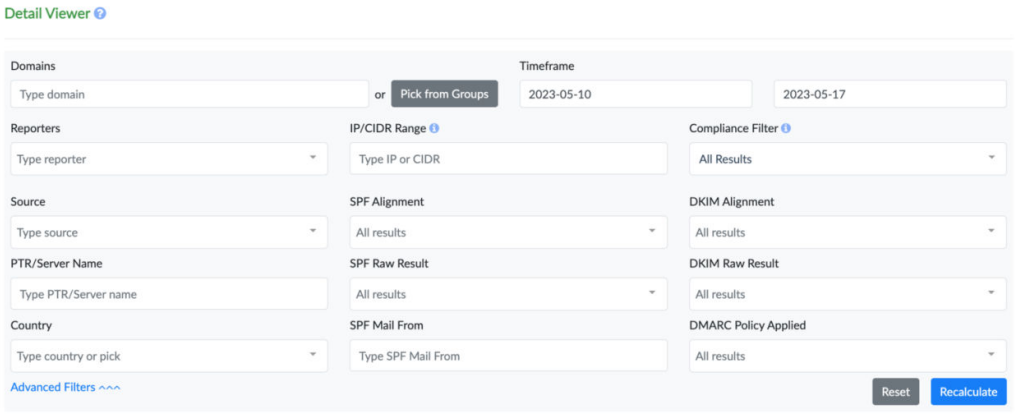
Una de las herramientas que brinda es para el análisis de los reportes RUA y RUF, de forma automatizada y centralizada. Con una interfaz web bastante amigable, se pueden ver los tráficos reportados en nuestro nombre desde dominios receptores en todo el mundo.



Tablero vista general de dominios con mapa (dmarcian) [12]



Tablero de tráfico monitoreado cumpliendo DMARC (dmarcian) [12]



Detalle de filtros para búsqueda de reportes DMARC (dmarcian) [12]

Si bien herramientas como esta ayudan a encontrar rápidamente los casos de desvíos en validaciones DMARC a investigar, luego cada uno se debe verificar manualmente para comprender si de trataron de un error de configuración de alguna de las partes, o si efectivamente son casos positivos de ataques de Spoofing.

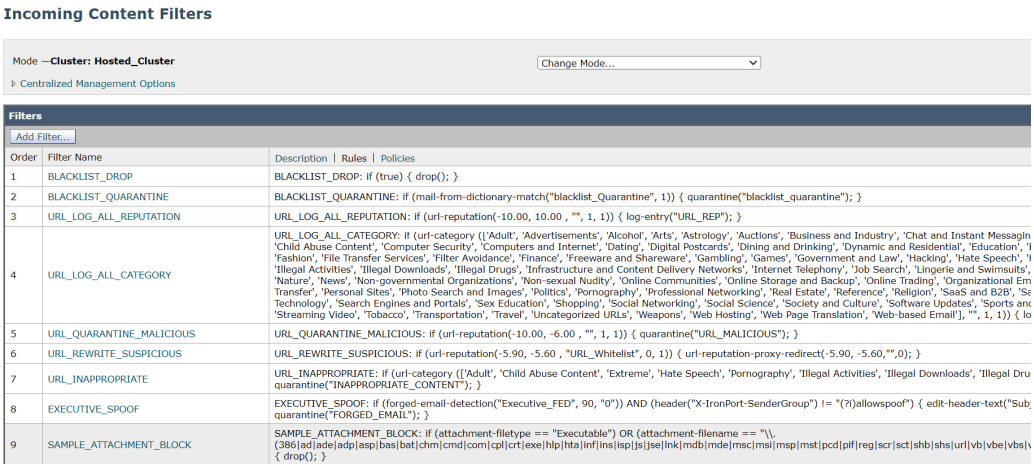
8.6 Reglas y Filtros de contenido avanzados

Hablamos antes de la gran potencialidad que brinda el módulo de Filtros de Contenido ("Content Filters"), para crear reglas y funciones propias, funciones que de alguna u otra forma están disponibles en varias soluciones de Gateway de correo, en este caso veremos la sintaxis propietaria de Cisco CES [7].

Los filtros de contenido se crean usando un lenguaje de programación sencillo, que tiene sentencias lógicas básicas, permite el uso de variables y cuenta con funciones predefinidas relacionada con el acceso a la toda la información disponible en un correo electrónico.

Se dispone también de un repositorio para crear de "diccionarios" propios, que son vectores de cadenas de texto constantes, o sea una lista de textos estáticos para hacer comparaciones o búsquedas en tiempo de ejecución.

Las reglas se ejecutan de forma secuencial de 1 a N, por lo que resulta importante ordenar las reglas de forma que se optimice el uso de procesamiento, por ejemplo colocando primero las que en caso de aplicar descartan el mensaje y cortan la ejecuciones posteriores, similar a lo que haríamos en un Firewall.



Vista de reglas en un flujo de ingreso de mensajes en Cisco CES

Por ejemplo, con la siguiente regla, se envía un email a una cuarentena llamada "quarantine_for_blacklist", cualquier correo cuyo origen ("from"), coincida con alguna de las entradas incluidas en el diccionario "blacklist_cust":

if (mail-from-diccionary-match("blacklist_cust",1))

{qurantine("quarantine_for_blacklist");}

Este es un ejemplo simple, en el cual sólo se hace uso de datos del encabezado del correo ("from"), pero también se puede operar con cualquier texto incluido en el cuerpo del correo.

8.6.1 Reglas avanzadas contra Phishing

Existen un grupo de funciones extremadamente útiles para combatir el Phishing, como por ejemplo las funciones "url-reputation" y "url-reputation-proxy-redirect".

Primero debemos entender la sintaxis de la función "url-reputation":

<filter_name>: If url-reputation('<min_score'>, <'max_score'>, '<allowedlist>', '<include_attachments>','<include_message_body_subject>')

{<action>}

Donde los parámetros son:

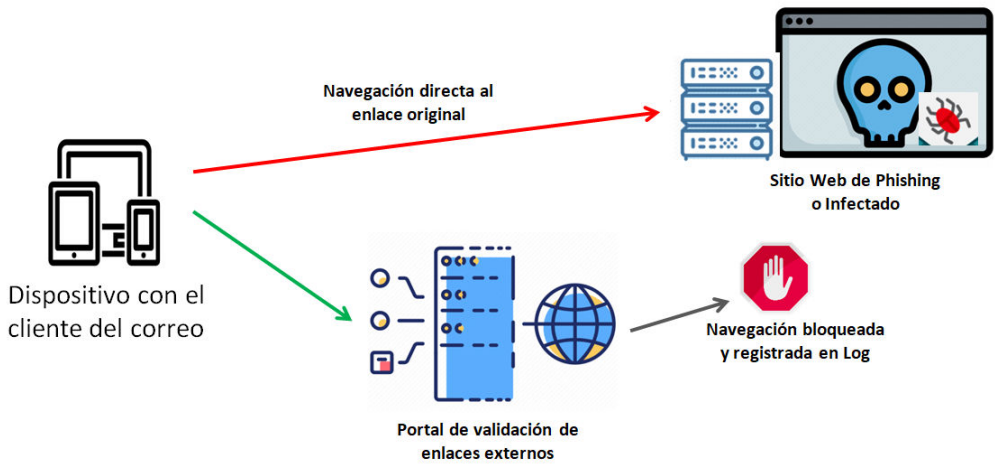
- filter_name: es el nombre del filtro
- allowedlist: es el nombre de una lista de URL permitidas definida de manera opcional
- min_score y max_score: son las puntuaciones mínimas y máximas en el rango para el que debe aplicarse la acción. Las mismas deben estar entre -10 y 10
- include_attachments: se utiliza para buscar direcciones URL en los archivos adjuntos del mensaje: 1 = activo; 0 = inactivo.
- include_message_body_subject: se utiliza para buscar direcciones URL en el cuerpo y el asunto del mensaje: 1 = activo; 0 = inactivo.

Usando como base esta función, creamos la siguiente regla que analiza cada URL que se encuentra el cuerpo de un correo, para re-direccionarla a un portal seguro en caso de que la reputación del destino sea sospechosa:

if (url-reputation (-5,-1, "URL_Whitelist", 0, 1))

{url-reputation-proxy-redirect(-5,-1,"",0);}

En este ejemplo las URL cuyo puntuación sea entre -5 y -1 (posiblemente maliciosas) se reescriben para que, si un usuario luego hace clic, se desvíen a un portal que actúa como protección al usuario. Así mismo se utiliza el diccionario URL_Whitelist para omitir del filtro dichas URL que ya se conocen como confiables a pesar de su puntuación.



Reemplazo de enlaces en correos por un salto a un portal seguro

Como vemos en sólo dos líneas, hemos agregado una protección significativa a todos los correos que recibe nuestra organización. La clave está en la gran potencia de las funciones, ya que en este último ejemplo lo que el sistema debe hacer es complejo. Por cada mail debe: abrir e interpretar la totalidad del contenido del mail buscando links a sitios web, consultar cada link web encontrado contra la base de reputación en Internet (en este caso "Talos"), hacer la comparación de puntaje y luego si corresponde modificar el contenido de cada correo para alterar el destino del link original.

8.6.2 Reglas avanzadas específicas contra BEC/Spoofing

Hay 2 funciones que nos resultan especialmente útiles para combatir los ataques de Spoofing que hacen uso de dominios "look-alike" (similares a la vista al real pero escrito diferente).

Repasando como se están realizando los ataques combinados de BEC/Spoofing, primero los atacantes logran obtener una cadena de correo auténtica haciendo alguno de los ataques de BEC (Business Email Compromise). Luego con esta cadena real, inician una nueva comunicación

a la víctima usando técnicas de Spoofing, muchas veces desde un dominio nuevo creado para este fin [2].

Ya que los atacantes deben registrar un nuevo dominio de correo que se vea similar a uno real, esto lo suelen hacer recién cuando tienen un objetivo en la mira, posiblemente luego de comprometer los datos de alguna cuenta de correo del objetivo.

Por lo que los atacantes tiene una ventana de tiempo limitada desde que comprometen una cuenta, registran un nuevo dominio para engaños y concretan el ataque de Spoofing. Esta restricción que ellos tienen, nos dará pie a nuestra principal forma de defendernos.

Las funciones que nos ayudan en esta tarea son:

- sdr-reputation:
  La función nos devuelve el nivel de categoría de reputación del emisor definido en 5 valores posibles: No confiable ("Untrusted"), cuestionable ("Questionable"), neutral ("Neutral"), favorable ("Favorable") y confiable ("Trusted").
- sdr-sender-maturity:
  La función nos devuelve la antigüedad que tiene el dominio emisor de correo, o sea la cantidad de tiempo que lleva activo desde que nació.

La regla general que recomiendo crear para prevenir estos ataques de Spoofing quedaría entonces así:

if (sdr-sender-maturity (“days”, <=, 90, “”) AND sdr-reputation ([‘neutral’,‘questionable’, ‘untrusted’], “”)) {qurantine("suspect_for_Spoofing");}

Es decir, que aquellos correos desde emisores que fueron creados hace menos de 3 meses, y que además no tienen una reputación claramente positiva, son enviados a una cuarentena denominada

"suspect_for_Spoofing", para ser revisados manualmente por personal de riesgos/seguridad informática.

Con esta simple regla estamos previniendo la gran mayoría de los ataques de BEC/Spoofing más comunes. Contando con la disponibilidad de un adecuado personal que puede estar atento a esta cuarentena, la reacción para bloquear los dominios de atacantes y comenzar la investigación puede ser casi inmediata.

También se puede optar por una táctica inicial mucho más agresiva, por ejemplo, enviando a cuarentena todos los mails desde dominios con menos de 180 días de antigüedad. Y en base a los resultados que se obtengan, ir adaptando los valores o agregar más condiciones a la regla. Pero dependerá del tamaño de la organización, tipo de industria y tipo de interlocutores que solemos tener.

8.6.3 Reglas avanzadas contra el compromiso de cuentas

Así como agregamos controles en el flujo de mensajes entrantes, para los mails salientes también podemos aplicar técnicas específicas para la detección de posibles cuentas internas comprometidas.

La identificación de que los controles de acceso que disponemos han fallado y que una cuenta de correo de nuestra organización ha sido tomada por un atacante, es una tarea difícil. Si el atacante que mantiene tomada la cuenta hace un uso discreto, dirigido e inteligente de la misma, será casi imposible detectarlo desde el Gateway de correo.

Pero muchos de los ataques masivos lo que intentan es usar las cuentas ya comprometidas para expandirse aún más, iniciando por ejemplo, mails con ataques de Phishing desde esta cuenta conocida hacia nuevas víctimas.

Lo que podemos hacer es crear una regla para que a cada correo saliente se le verifique si contiene una URL que tiene una reputación

clasificada como maliciosa (negativa). En ese caso hacer una copia del correo saliente en una cuarentena, y darle un aviso automático a personal de seguridad informática para que lo analice e investigue si el mail fue generado por el usuario, o si la cuenta está efectivamente comprometida y está intentando iniciar ataques desde ésta. La regla podría quedar así:

if (url-reputation (-5,-1, 0, 0, 1))

{ duplicate-quarantine("suspect _for_compromise")

notify ("seginf@ejemplo.com", "Possible account compromise", "", "Account sending malicious URLs");}

Es importante siempre enviar una copia a cuarentena los correos saliente que nos interesa revisar, porque los atacantes o malware inmediatamente borran los correos que generan y no queda ninguna evidencia visible del lado del cliente de usuario comprometido.

Reglas similares podrían adicionarse para detectar cualquier correo que nuestra organización intente enviar que contenga adjuntos con virus o malware, etc.

9 Las próximas tendencia de la seguridad de correo

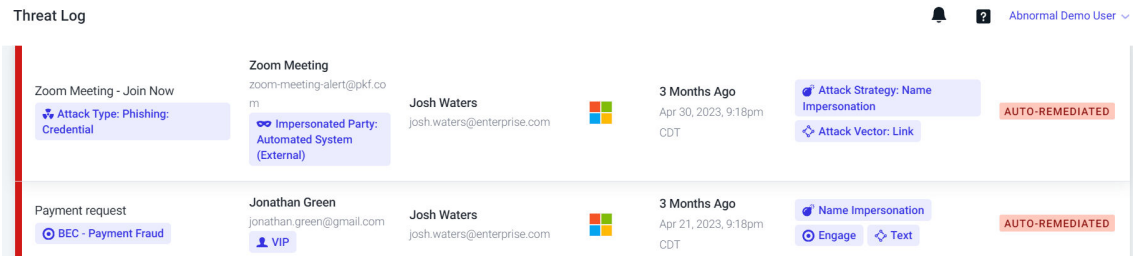
Hemos visto con detalle cómo funcionan los Gateway de correo actuales y las enormes posibilidades que nos brindan para elevar sustancialmente el nivel de seguridad de nuestra infraestructura de correo.

Pero la evolución de la seguridad ya está mostrando nuevas tendencias que avanzan principalmente en el análisis de contenido usando técnicas cada vez más avanzadas a los efectos de encontrar patrones comunes de ataques conocidos.

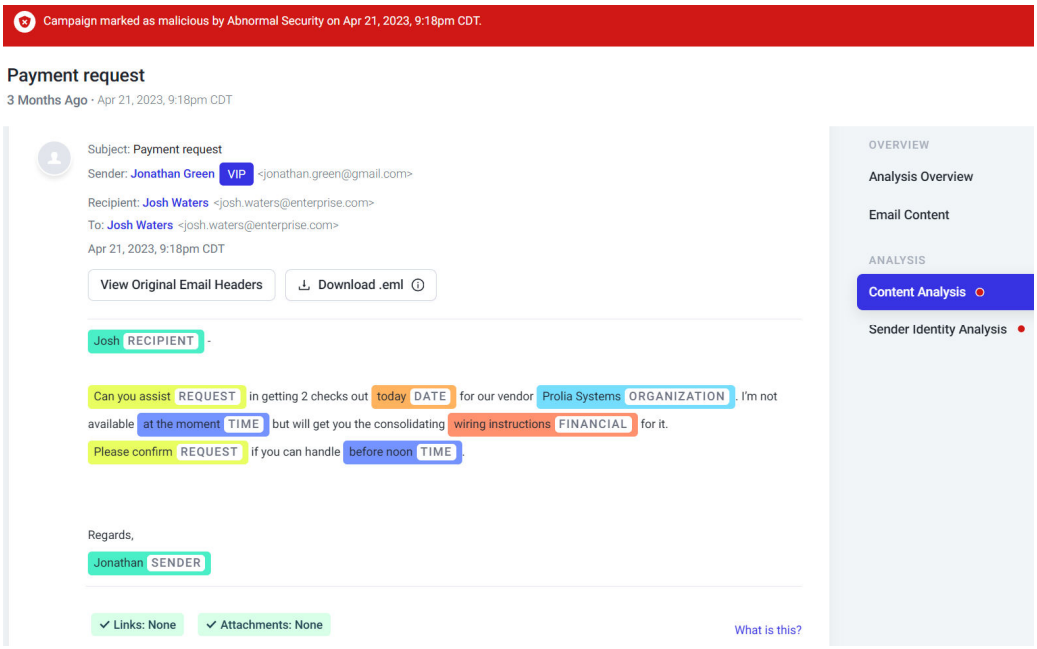
Como ejemplo de lo que está por venir, en junio del 2023 Cisco completó la compra de la compañía "Armorblox". La empresa se especializa en sistemas de protección del correo electrónico y otras aplicaciones de escritorio, que funcionan con tecnología de inteligencia artificial o "AI" para la comprensión del lenguaje natural o NLU ("Natural-language understanding") [13].

Tanto Proofpoint como CheckPoint afirman que ya están utilizando técnicas de "AI" dentro de sus productos de soluciones de protección de correo. Afirman que los utilizan dentro de sus sistemas de análisis de amenazas en la nube, los que tienen como salida los valores de las puntuaciones de reputación de sito y dominios emisor que reciben sus clientes en el Gateway de correo [14] [15].

Abnormal Security parece estar más avanzada al brindar varios tableros de reportes sobre los comunicaciones que fueron analizadas usando "AI" y resultaron identificadas como posibles amenazas conocidas en base a patrones que coinciden con el aprendizaje que efectuó sobre el comportamiento de cada usuario [16].



Captura de Demo de Abnormal AI Security Mailbox identificando ataques Phishing y BEC [17]



Captura de Demo de Abnormal AI Security Mailbox analizando contenido usando "NLU" [17]

En una demo de la solución Abnormal AI Security Mailbox se puede ver el análisis de contenido y la clasificación que realiza de cada dato dentro del texto de la conversación, para poder concluir la intencionalidad u objetivo del correo del emisor [17].

Sin embargo, ningún proveedor brinda detalles de exactamente como son sus sistemas "AI", lo que despierta sospechas de cuánto de novedoso tienen sus tecnologías y cuánto sigue funcionando con lo que antes denominamos técnicas analíticas o estadísticas clásicas. Los servicios en la nube (cloud SaaS) proporcionan un nivel de ocultamiento ideal para promocionar y hacer marketing de tecnologías que tal vez tienen un impacto mínimo en el funcionamiento real.

Por el movimiento que se ve de adquisiciones y fusiones, es evidente que los grandes jugadores están haciendo enormes inversiones en investigación y desarrollo del AI aplicado a seguridad.

Pero es imposible llegar a analizar o emitir conclusiones de una tecnología tan reciente, en la que mayormente se tratan de anuncios y

proyectos de desarrollos casi experimentales y donde el secreto industrial es tan cerrado.

9.1 Como funcionaría la protección basada en AI

Como no podemos tener acceso a conocer cómo estarían operando internamente estas primeras soluciones de mercado, podemos inferir cuáles serían las bases de su funcionamiento.

Los sistemas estarían basados en el entrenamiento permanente de redes neuronales que obtienen un resumen del contenido de cada correo emitido y recibido por cada usuario. Para obtener el resumen se podrían utilizar criterios de agrupación de tipo de contenido por número de palabras clave relacionados a cada temática, así como también patrones basados en frases clave (oraciones) para brindar mayor contexto al sistema de ponderación lingüístico aplicado.

Estos comportamientos normales de usuarios de nuestra organización, se compararían con patrones obtenidos del aprendizaje de casos en los que la "AI" fue entrenada por el proveedor de seguridad con ataques reales o típicos de BEC/Spoofing, Phishing e ingeniería social.

Si un usuario presenta una anomalía en su patrón normal de comunicación y este coincide, dentro de un margen de confianza suficiente, con un patrón conocido de ataque definido por el proveedor, el sistema lo alertaría identificando el tipo de coincidencia obtenida.

Por supuesto los patrones de comportamiento aprendidos en cada organización cliente, terminarían alimentando la "AI" única del proveedor, lo que brindaría una protección evolutiva permanente para todos los usuarios de la solución.

10 Los riesgos de confidencialidad en el control del correo

La medidas de seguridad que se basan en el monitoreo o inspección, siempre impactan en la privacidad y confidencialidad. Desde las cámaras de seguridad en la calle, oficina o en una residencia, al análisis de la navegación en Internet en un proxy.

Pero en el caso puntual de las comunicaciones por correo electrónico, estamos hablando de uno de los medios generalmente más utilizados en la práctica para la transmisión de datos clasificados, privados y altamente confidenciales.

En las soluciones de Gateway de correo convencionales, el mayor riesgo de que información confidencial escape de los destinatarios definidos se da con el uso de las cuarentenas. Es decir aquellos correos que por algún motivo personal de IT, de riesgos o de seguridad informática debe revisar de forma manual. Por eso hay que ser muy cuidadoso en las reglas de cuarentena que se crean, y quienes van a ser la personas con acceso a la revisión de estos correos retenidos.

En esos sistemas convencionales durante el control normal de contenido y adjuntos, ya sea el de antivirus, filtros de contenidos, o reglas personalizadas que hayamos creado, no se almacena información del contenido de los correos. Es decir la información se accede de forma de forma completa para ser analizada automáticamente, pero una vez terminado el análisis se cierra el correo y no se almacenan datos de su contenido.

10.1 Los riesgos en el uso de soluciones de "AI"

Con las soluciones de "AI" el escenario es diferente al que veníamos aplicando hasta ahora, ya que estarían basando parte de su aprendizaje en el análisis de las conversaciones, es decir, en el contenido de cada mail. Esto quiere decir que parte del contenido (no importa que tan resumido sea

el extracto o resumen que resulte), se está brindando para alimentar un sistema de datos administrado por un proveedor de seguridad.

Mientras mayores sean los requerimientos de interpretación del contenido de correos para brindar mayor seguridad, mayor será el tamaño de estas estructuras o bases de datos. El riesgo de pérdida del control en la confidencialidad es más que evidente. Estamos entregando una copia de la información de nuestra organización a un tercero, que a su vez la usa para mantener el sistema funcionando en otros clientes que podrían ser empresas competidoras, organismos de regulación, gobiernos de estados extranjeros, organizaciones de dudosa reputación, etc.

El perfilamiento detallado del comportamiento de cada usuario en base a sus comunicaciones privadas podría tener un nivel de información tan crítico que sería potencialmente peligroso incluso para el uso interno.

Mientras esta información esté almacenada por el proveedor, y sea de cierta forma indirecta usada o "compartida" con los demás clientes, siempre se estará sumando el riesgo adicional de fuga, filtraciones, compromiso, ataques a la "AI" [18], etc.

Para avanzar con el uso de estas tecnologías hay que ser extremadamente cauteloso en que información se está brindando, con qué propósito, cómo se procesa y que políticas de confidencialidad se mantienen. Requerimientos básicos que parecen difíciles de poder cumplir considerando el actual nivel de hermetismo con el cual estas primeras soluciones de "AI" en la nube se están ofreciendo en el mercado.

Conclusiones

El correo electrónico nació como un mecanismo de comunicación casi sin diseño de seguridad, cuando no se podía tener noción del crecimiento que iba a tener en el futuro y del uso específico al que se le iba dar en la actualidad.

Los protocolos de seguridad de correo que se sumaron posteriormente para mejorar la seguridad de SMTP, en concreto: SPF, DKIM y DMARC, sorprendentemente no se encuentran aún implementados en muchas organizaciones. Mientras esto perdure la prevención rigurosa del Spoofing resulta prácticamente imposible [2].

La aparición del Gateway de correo electrónico marcó un significativo avance a la seguridad, especialmente cuando es nutrido con sólidas bases de datos de dominios emisores. La información del tiempo de vida y reputación de los dominios se convirtió en clave para la identificación y filtrado de contenido, aunque pocas organizaciones hacen un uso inteligente de los mismos.

Pasos para la prevención de BEC/Spoofing

Para la prevención de los ataques de Spoofing, especialmente los más peligrosos que son los que suelen iniciarse luego de la obtención de un correo mediante técnicas de BEC, es necesario primero garantizar el correcto funcionamiento de los protocolos SPF y DKIM, gobernados por DMARC.

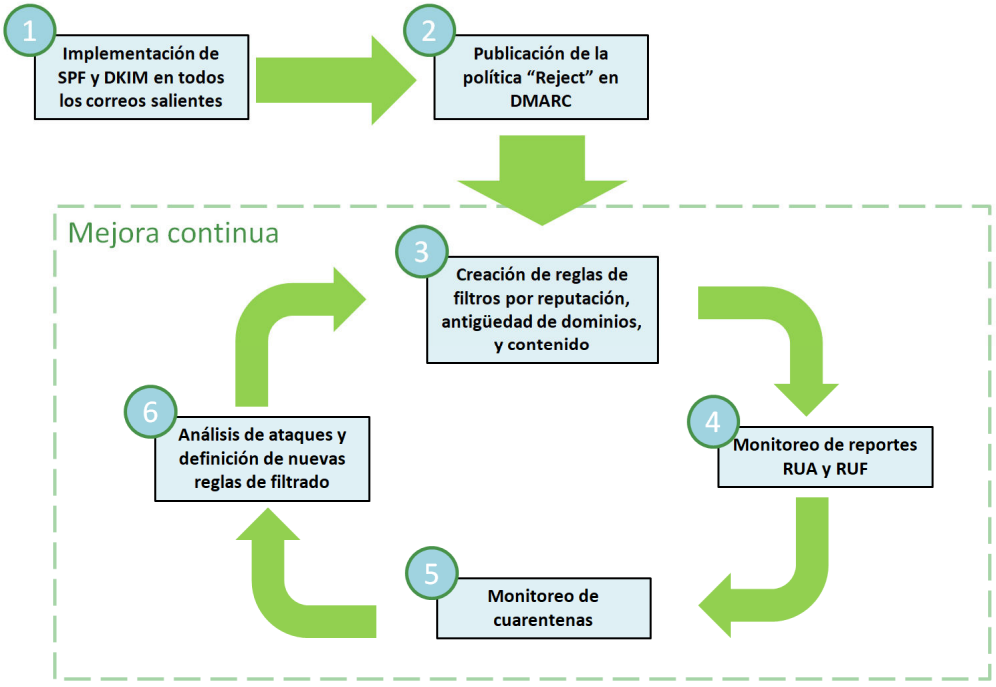
Para lograrlo, primero aplicamos con DMARC una política de monitoreo "None", y vamos analizando las fallas que tengamos en SPF o DKIM hasta corregir la totalidad de nuestra infraestructura de correo. Una vez que tenemos la infraestructura en orden, pasamos a una política "Quarantine", y verificamos durante un tiempo (por ejemplo 2 meses) que no se produzcan más desvíos en los controles que nos informan nuestros receptores de correos.

Luego de este plazo de prueba, aplicamos de forma definitiva una política DMARC segura para nuestra organización, lo que protege nuestra reputación y nos escuda legalmente de cualquier reclamo de terceros que sean victimas fuera de nuestro ámbito de control directo.

Recién cuando todos los interlocutores habituales de las comunicaciones con una organización han llegado a aplicar una política DMARC "Reject", que es la única segura, podríamos decir que estamos en un entorno "DMARC compliant".

Si bien las técnicas de defesa contra el Spoofing basado en el uso de Gateway de correo (SEG) descriptas en el presente trabajo funcionan en cualquier tipo de ambiente, ya sea en uno favorable o adverso, su efectividad será mucho mayor si estamos operado en un entorno "DMARC compliant".

En un entorno seguro, las reglas avanzadas de filtros de contenido basadas en reputación y tiempo de vida de cada emisor, deberían poder detener casi todos los intentos de suplantación más habituales.



Circuito conceptual propuesto para la prevención del BEC/Spoofing

Conclusiones finales

Como hemos visto el Gateway de correo electrónico (SEG) se ha convertido en un aliado indispensable para asegurar el perímetro de comunicaciones de las organizaciones.

El correo electrónico sigue siendo el principal medio desde donde se inician, posiblemente, la mayoría de los ataques en ciberseguridad. Ya sea usando técnicas de ingeniería social, de Phishing para robo de credenciales o información, distribución de Virus y Malware (incluyendo "ransomware"), fuga de información sensible, publicación de información clasificada, Spam, campañas de difamación, etc.

A los anteriores hay que sumarle específicamente el ataque combinado de BEC/Spoofing que es uno de los que mayores pérdidas represen cada año (totalizando casi 3 mil millones de dólares sólo en Estados Unidos durante el año 2023 [1]).

Espero que este trabajo, en conjunto con el de "Ataques y protección en el servicio de correo electrónico" [2], presentado anteriormente, ayuden a tener una renovada perspectiva de la seguridad en correo electrónico. Entendiendo no sólo cómo llegamos a la situación actual en la que, como vimos en el trabajo anterior, importantes organizaciones de todo tipo aún no están cumpliendo con los estándares básicos de seguridad del correo (visibilizados por DMARC), pero más que nada para describir que pasos, técnicas y tecnologías actualmente disponibles podemos implementar para corregir y mejorar nuestra postura de seguridad.

Objetivos que veo totalmente alcanzables al combinar el cumpliendo los estándares de seguridad de correo emitidos por la Internet Engineering Task Force's (IETF), específicamente SPF, DKIM y DMARC, haciendo un uso exhaustivo e inteligente de un Gateway de correo (SEG) actual, y manteniendo un adecuado esquema de monitoreo que impulse la mejora continua.

El uso combinado de estas técnicas deberían detener la mayoría de los intentos de ataques más comunes de suplantación actuales, y con ellos gran parte de otros ataques vía correo electrónico caracterizados por este virtual anonimato de origen con el cuál nació el primer protocolo hace ya más de 40 años. Por supuesto, en el momento que todas las organizaciones logren alcanzar este nivel de seguridad en sus infraestructuras de correo, probablemente los atacantes buscarán nuevos vectores y metodologías que sean efectivos para lograr su objetivo. Pero esa será una batalla para el futuro.

Bibliografía

[1] Internet Crime Complaint Center (IC3) Federal Bureau of Investigation (FBI), "Internet Crime Report 2023" (Abril 2024) Disponible en: https://www.ic3.gov/Media/PDF/AnnualReport /2023_IC3Report.pdf (Consultada el 04/06/2024)

[2] Corbellini Claudio, "Ataques y protección en el servicio de correo electrónico", Trabajo final de especialización en Seguridad Informática de la Universidad de Buenos Aires (Abril 2024)

[3] Cisco Systems, "Cisco Announces Agreement to Acquire IronPort". (Enero 2007). Disponible en: https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2007/m01/cisco-announces-agreement-to-acquire-ironport.html (Consultada el 01/03/2024)

[4] Info Tech Research Group 2024, Software Reviews, "Cloud Email Security Data Quadrant 2023". Disponible en: https://www.softwarereviews.com/ awards/data-quadrant-awards-2023-cloud-email-security (Consultada el 06/05/2024)

[5] Cisco Talos Intelligence Group, "About Talos". Disponible en: https://www.talosintelligence.com/about (Consultada el 06/04/2024)

[6] Talos, "Domain Reputation Overview": https://www.talosintelligence.com/reputation_center/lookup?search=mit.edu (Consultada el 07/05/2024)

[7] Cisco Systems "User Guide for AsyncOS 14.2 for Cisco Secure Email Cloud Gateway - GD" (2022) Disponible en: https://www.cisco.com/c/en/us/td/docs/security/esa/esa14-2/user_guide/b_ESA_Admin_Guide_14-2.html (Consultada durante el primer semestre de 2024)

[8] Cisco Systems "Advanced Malware Protection on Cisco Email Security". Disponible en: https://www.cisco.com/c/dam/global/th_th/assets/docs/seminar/AMP_ESA.pdf (Consultada el 11/05/2024)

[9] Alex Chan, "Best Practice Guide for Anti-Spam, Anti-Virus, Graymail and Outbreak Filters - Cisco Secure Email Gateway" (Cisco Systems 2020) - Cisco Document ID:215164 Disponible en: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/215164-best-practice-guide-for-anti-spam-anti.html (Consultada durante Abril 2024)

[10] Alex Chan, "Best Practice Guide for Advanced Malware Protection (AMP) on Cisco Email Security" (Cisco Systems 2020) - Cisco Document ID: 215165 Disponible en: https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/215165-best-practice-guide-for-advanced-malware.html (Consultada durante Abril 2024)

[11] Cisco Systems, "Cisco Secure Email + dmarcian" (Diciembre 2021): Disponible en: https://docs.ces.cisco.com/docs/dmarcian-cisco-secure-email (Consultada el 12/05/2024)

[12] dmarcian, "Getting started with dmarcian" (Septiembre 2021): Disponible en: https://dmarcian.com/getting-started-with-dmarcian/ (Consultada el 12/05/2024)

[13] Eduard Kovacs, "Cisco Acquiring Armorblox for Predictive and Generative AI Technology" - SecurityWeek (Junio 2023) Disponible en: https://www.securityweek.com/cisco-acquiring-armorblox-for-predictive-and-generative-ai-technology (Consultada el 25/05/2024)

[14] Proofpoint Inc, "How Proofpoint Uses AI" - What Is Artificial Intelligence? Disponible en: https://www.proofpoint.com/au/threat-reference/artificial-intelligence (Consultada el 26/05/2024)

[15] Check Point Software Technologies Ltd., "Why You Must Have AI For Email Security" - CheckPoint Cyber Hub. Disponible en: https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-email-security/why-you-must-have-ai-for-email-security (Consultada el 26/05/2024)

[16] Abnormal Security, "AI Security Mailbox" - Abnormal Security Products: https://abnormalsecurity.com/products/ai-security-mailbox (Consultada el 27/05/2024)

[17] Abnormal Security, "Why Abnormal" - Interactive demo Disponible en: https://abnormalsecurity.com/tours/why-abnormal (Consultada el 28/05/2024)

[18] Apostol Vassilev, Alina Oprea, Alie Fordyce y Hyrum Anderson, "Adversarial Machine Learning" - NIST AI 100-2 (Abril 2024) Disponible en: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-2e2023.pdf (Consultada el 08/06/2024)