centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1636

Procedimiento de empleo seguro
Email Protection y Targeted Attack Protection

Abril 2024

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

Pº de la Castellana 109, 28046 Madrid.

NIPO: 083-24-149-6.
Fecha de Edición: abril 2024.

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.04.12 10:11:42 +02'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1 INTRODUCCIÓN

1. Proofpoint tiene como objetivo proporcionar una plataforma que permita la protección frente a amenazas básicas y avanzadas de correo, así como la posibilidad de eliminar o enviar a cuarentena correos electrónicos malintencionados que se han recibido en las bandejas de entrada de los usuarios.

2. Dicha plataforma ofrece las siguientes capacidades:

   - Protección frente a amenazas básicas de correo electrónico entrante y procedente del exterior:
     - Protección frente a campañas de spam y masivo.
     - Protección frente a correo recibido de fuentes desconocidas que no superen los estándares de autenticación SPF, DKIM y DMARC.
     - Protección frente a suplantación de identidad.
   - Protección frente a amenazas avanzadas de correo entrante y procedente del exterior:
     - Análisis en un entorno aislado (*sandboxing*) de URLs incluidas en los correos para determinar la existencia de malware o phishing antes de la entrega de los mismos en la bandeja de entrada de los usuarios, así como después de su entrega.
     - Análisis en un entorno aislado (*sandboxing*) de adjuntos incluidas en los correos para determinar la existencia de malware o phishing antes de la entrega de los mismos en la bandeja de entrada de los usuarios.

3. La plataforma de protección frente a amenazas de Proofpoint, cuenta con dos componentes que trabajan en conjunto. En un primer nivel, se dispone de la herramienta Email Protection, que permite realizar ciertas tareas de detección y bloqueo, y se complementa con TAP (Targeted Attack Protection), que se centra en la detección de amenazas avanzadas.

1.1 FILTRADO DE CORREO

4. La plataforma de Proofpoint permite tener flujos e incluso políticas separadas tanto para correo entrante como correo saliente de la organización.

5. Además, dispone de distintas capas de filtrado entre las que encontramos:

   - Análisis de reputación dinámica para direcciones IP y dominios continua (Proofpoint Dynamic Reputation Service).
   - Detección de malware con tecnología de varios antivirus incorporada (F-Secure y McAfee), incluso cuando se trata de un adjunto comprimido y protegido con contraseña (se busca la contraseña en el cuerpo del mensaje).
   - Uso de estándares de autenticación de correo SPF, DKIM y DMARC, pudiendo configurar de forma flexible e individual para cada caso concreto, y con la posibilidad de incorporar firmas DKIM para emitir correos firmados salientes de la plataforma.
   - Configuración de filtros ad-hoc, estableciendo políticas y configuraciones con más de 50 atributos disponibles (archivo corrupto, nuevo dominio, cabeceras, sender, idioma detectado, etc.).

1.2 ACCIONES

6. Cuando se caracteriza cualquier flujo de correo, se pueden llevar a cabo distintas acciones automáticas. Además, las acciones a realizar no son excluyentes. Es posible añadir cualquier correo a una carpeta de cuarentena (se guarda una copia del mismo en una carpeta, sin restricción por número de carpetas) mientras que se sigue procesando, rechazando o cifrando. Se pueden hacer acciones de añadir destinatarios, cambios de asunto, cambios de cabeceras, redirecciones, emitir alertas, etc.

1.3 DETECCIÓN DE AMENAZAS MULTICAPA

7. Mediante distintas capas de clasificadores de correos electrónicos dinámicos, Proofpoint permite categorizar los correos como phishing, malware, spam, correo masivo (bulk), contenido de adultos, impostor (BEC), fraude o círculo de confianza, entre otros, usando MLX o técnicas de machine learning avanzadas, usando la red de inteligencia de Nexus Threat Graph.

8. Empleando un amplio rango de métodos tradicionales de detección (técnicas bayesianas y heurísticas) y algoritmos machine learning, el motor de análisis se ajusta dinámicamente sin la necesidad de intervención manual. Como resultado, el motor MLX de Proofpoint ofrece clasificación y protección en tiempo real con unos niveles de eficiencia situados en más del 99,8%.

9. Además, dispone de un enfoque totalmente novedoso, enfocado en la detección y bloqueo de las amenazas más sofisticadas, utilizando un motor de aprendizaje automático SCSS (Stateful Composite Scoring Service), que se entrena automáticamente y mejora los ratios de detección a partir del correo que procesa la propia plataforma de la compañía, a partir de correos que se clasifican inicialmente como no deseado. Este motor, usado junto con el motor de clasificación MLX produce una puntuación neta para cada correo procesado por la plataforma y cada clasificador (spam, bulk, phish, adult, etc.) y aumentando el ratio de detección de correo no deseado por encima del 99,9%.

10. Con estas técnicas englobadas en la detección Supernova de Proofpoint, los ataques de impostor (fraude del CEO) se ven bloqueados de forma proactiva, utilizando inteligencia para la lectura de cabeceras, establecer la reputación del enviador (dominios, direcciones IP), analizar la relación de confianza con el enviador y el destinatario (Circle of Trust), analizar el contenido (metonimios, frases frecuentes y de estafa, detección de sentido de urgencia, etc.).

1.4 DETECCIÓN DE AMENAZAS AVANZADAS

11. A través de la funcionalidad Targeted Attack Protection (TAP), Proofpoint ayuda a detectar, mitigar y bloquear amenazas avanzas que llegan a través del correo, incluyendo los ataques que usan URLs y adjuntos maliciosos para instalar malware o engañar a los usuarios y conseguir que compartan contraseñas e información sensible.

12. Mediante la verificación estática de los hashes de archivos adjuntos, TAP puede discernir si un fichero es malicioso o no. En caso de que no haya sido previamente analizado y no se disponga de dicha información, se realiza un análisis dinámico en un entorno aislado y de pruebas (*sandbox*) de Proofpoint, observando su comportamiento, la existencia de malware, el código utilizado o incluso los protocolos, obteniendo un veredicto de su

benignidad o maliciosidad, para poder bloquearlo o no. Todo lo que se aprende a través del *sandbox*, se incorpora a la red de inteligencia reputacional, para poder dar una respuesta más rápida.

13. En el caso del análisis de las URLs que se encuentran en los correos (explícitas o no), se analizan de la misma forma que los ficheros adjuntos, utilizando su reputación. En caso de que no se conozcan, se reescriben, de forma que se incorpora un sufijo (urldefense.proofpoint.com) a la URL, y se analiza en un entorno controlado y aislado de Proofpoint (*sandbox*). En caso de ser maliciosa, se bloqueará.

14. En cualquier caso, al estar reescrita la URL, cuando un usuario dispone del correo en su buzón y hace *click* sobre la misma, realmente hará *click* sobre la reescritura, permitiendo un análisis en tiempo real y nuevo de la URL en cuestión. De esta forma, las URLs se siguen analizando continuamente incluso después de haber sido entregados los correos.

1.5 DETECCIÓN DE AMENAZAS SAAS

15. Con TAP se realiza de forma automática, la inspección de archivos de las aplicaciones en la nube, en busca de cuentas comprometidas a través de *logins* sospechosos, aplicaciones de terceros de riesgo, o incluso la existencia de ficheros compartidos de forma externa o interna y masiva.

2 OBJETIVO Y ALCANCE

16. El presente documento o guía, se desarrolla para la solución de protección de correo de *Proofpoint Email Protection y Targeted Attack Protection*. Se centra en la configuración segura de la solución, por lo que no cuenta con información detallada de instalación y configuración de elementos adicionales.

17. Este producto ha sido cualificado e incluido en el Catálogo de Producto y Servicios TIC (CPTSIC) en la familia “Protección de correo electrónico”.

3 ORGANIZACIÓN DEL DOCUMENTO

18. Este documento se compone de los siguientes apartados:

a) Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.

b) Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

c) Apartado **6**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

d) Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

19. Proofpoint realiza la provisión de recursos para ofrecer la plataforma de protección de correo Email Protection y Targeted Attack Protection en formato SaaS ofreciendo el acceso a los sistemas a través de un acceso web (URL).

20. La información acerca del acceso de la consola de administración, así como los datos de interés para realizar la integración con el flujo de correo existente, se realiza a través de un email. Este mensaje, se realiza desde una dirección de Proofpoint (**fulfillment@proofpoint.com**) y con destinatario, la persona contacto del cliente y asunto, "**[encrypt] Proofpoint on Demand Deployment Information**".

21. El mensaje se encuentra cifrado a través de la plataforma Email Encryption de Proofpoint. El usuario destinatario podrá acceder a la información a través del link "*Click here*" para acceder a la interfaz web de **Secure Reader** de Proofpoint para mensajes cifrados, donde podrá registrarse con su cuenta de correo, utilizar unas credenciales creadas previamente, o recuperar su contraseña en caso de olvido (vía email).

22. Es importante comprobar la validez de los certificados de los sitios web a los que se accede durante este proceso para asegurarnos que el servicio es legítimo y proporcionado por "proofpoint.com".

23. A continuación, se muestran unas imágenes orientativas:

Ilustración 1: Correo para realizar la autenticación

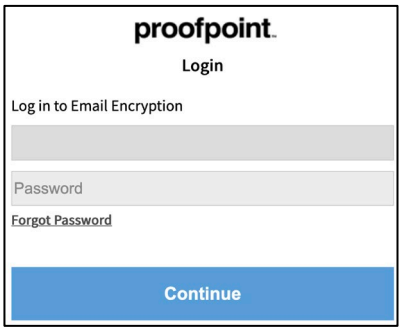

Ilustración 2: Interfaz de autenticación

24. El mensaje enviado, también incluye un fichero adjunto en formato .html, que permite leer la información haciendo clic en "*Click to read message*" e introduciendo las credenciales de Secure Reader.

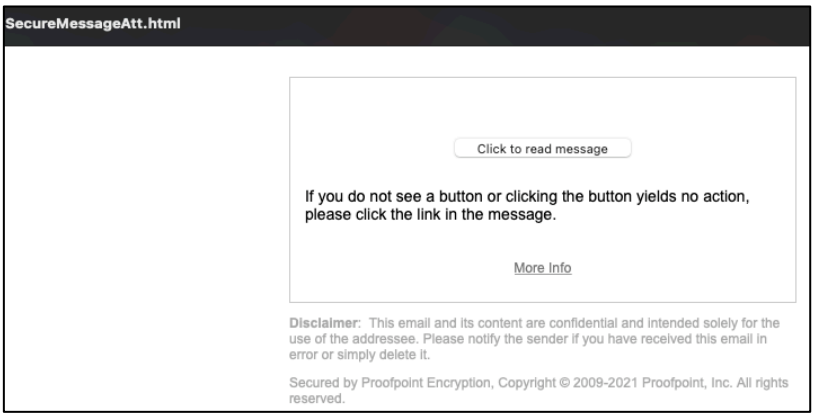

Ilustración 3: Correo con fichero HTML adjunto

25. La información proporcionada será de la siguiente manera (personalizado en cada caso):

Proofpoint on Demand - Enterprise

##################################

Welcome XXXX!

Thank you for using Proofpoint on Demand Enterprise.

Based upon the information you have provided, we have created a profile for your organization and are ready to start filtering and managing your email.

The following provides information on how to access your service.

Proofpoint Administrative GUI

address: https://XXXX.pphosted.com:10000

login: podadmin

password: XXXX

These passwords should be changed on your first login.

Proofpoint on Demand Enterprise - End User GUI (if enabled)

https://XXXX.pphosted.com:10020

A random default password has been set for end-user access. You may reset the default password in Groups and Users/Profiles/<PPS or other profile>/Advanced, or you may set up PPS to use an external authorization source.

NOTE: The administration and end-user web applications are reached via the ports above. If your company blocks non-standard ports at the firewall, you will need to create an exception for these ports.

MX Records

==========

Please change your public DNS entries to the following records (note the trailing "."!):

<yourdomain.tld>. 1800 IN MX 10 mxa-XXXX.gslb.pphosted.com.

<yourdomain.tld>. 1800 IN MX 10 mxb-XXXX.gslb.pphosted.com.

Repeat for each domain you route through Proofpoint on Demand. Note that the Proofpoint on Demand service must be configured for any additional domains prior to routing mail through it. All domains listed on your Pre-Deployment Questionnaire have already been configured.

Firewall Settings - Inbound

==========

Please allow port 25 (SMTP) access to your mail servers(s) from the following hostnames/IPs. These are your dedicated "Virtual IP" (VIP) addresses:

mx0X-XXXX.pphosted.com. X.X.X.X

mx0X-XXXX.pphosted.com. X.X.X.X

NOTE: If you do not restrict your firewall to allow only incoming mail from the Proofpoint on Demand service, you will likely receive mail sent directly to your mail server which will not be filtered by Proofpoint on Demand. This may cause your end users to believe that spam is getting through Proofpoint filtering, when in reality the messages are not being scanned at all.

It is recommended that after you configure your firewall, you contact your Proofpoint Sales Engineer to assist with testing mail flow from Proofpoint on Demand prior to changing your MX records.

If you have requested that your service be configured for regular LDAP imports, you will also need to provide either port 389 (LDAP) or port 636 (LDAPS) access to your LDAP or AD server from your Proofpoint Virtual IPs.

Outbound Mail Configuration

==========

If you are sending mail outbound through your Enterprise deployment, please send mail to the following hosts:

mxa-XXXX.gslb.pphosted.com

mxb-XXXX.gslb.pphosted.com

For redundancy, you must list all hosts by hostname in your outbound mail configuration, in a round-robin or ordered fashion. Please do not hard-code the IP addresses for these hosts, as it will impact our ability to provide you with the best redundancy possible.

Sender Policy Framework (SPF) Records

==========

If you are sending outbound mail through Proofpoint on Demand, it is very important that you modify your domain's DNS TXT records to include an "SPF" record for your domain. An SPF record is a way for a receiving mail system to determine if a sending server should be considered valid for the address listed in the "From" header. Without these records, some recipients (including AOL) may rate control or otherwise limit connections from Proofpoint's servers because the servers are part of Proofpoint's network, rather than your organization's.

A simple way to make this change is to add the following as a DNS TXT record to your domain:

"v=spf1 include:spf-XXXX.pphosted.com ~all"

You can, of course, add any additional values in your SPF records as necessary. By using the "include" syntax, we will be able to dynamically serve the addresses used for your cluster and keep it up to date for you with no maintenance required on your part.

For more information on SPF records, you can refer to the OpenSPF site: http://www.openspf.net/

The "include" syntax is specifically described here: http://www.openspf.net/SPF_Record_Syntax#include

Further Information

==========

Please login to the Proofpoint Customer Success Center to access key resources:

* Customer Support

* Product Discussion Forums

* Knowledge Base Access

* Admin Guides and Release Notes

* Online Case Tracking and Updates

* News Channels

https://proofpointcommunities.force.com/community/

4.2 ENTORNO DE INSTALACIÓN SEGURO

26. Proofpoint ofrece la plataforma de protección de correo Email Protection y Targeted Attack Protection en formato SaaS (Software as a Service) mantenido con recursos gestionados por Proofpoint, por lo que no se necesita la instalación de componentes adicionales.

4.3 REGISTRO Y LICENCIAS

27. Proofpoint ofrece la plataforma de protección de correo Email Protection y Targeted Attack Protection en formato SaaS (Software as a Service) por lo que no se realiza una gestión de licencias por parte del cliente. Éstas, se encuentran aplicadas en su entorno de producción, y son gestionadas por Proofpoint.

4.4 CONSIDERACIONES PREVIAS

28. Proofpoint ofrece la plataforma de protección de correo Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, por lo que no se necesita realizar consideraciones previas acerca de componentes adicionales o modelo de arquitectura.

29. Se deberán tener en cuenta los requisitos de los puestos de trabajo que accederán a la plataforma para administrarla, y que puede encontrar resumidos a continuación:

    - Navegador web soportados: Mozilla Firefox, Google Chrome, Internet Explorer 11, Microsoft Edge, Safari; en las versiones mantenidas por los propios fabricantes.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

30. Proofpoint Email Protection y Targeted Attack Protection pueden disponer de elementos externos para su uso extendido, como, por ejemplo, autenticación externa (sistema SAML) o entornos de correlación y guardado de eventos externos (como sistemas SIEM y similares). Ninguno de estos componentes es necesario para el uso de forma segura de la plataforma de Proofpoint.

5 FASE DE INSTALACIÓN

31. Proofpoint ofrece la plataforma de protección de correo Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, por lo que no se necesita la instalación de componentes adicionales.

6 FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

32. Proofpoint ofrece la plataforma de protección de correo Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, por lo que no se necesita ninguna configuración específica para operar en el modo de cumplimiento *Common Criteria*.

6.2 AUTENTICACIÓN

33. El mecanismo de autenticación de usuarios de Email Protection es mediante credenciales locales en la propia plataforma, es decir, usando un usuario consistente en un nombre para su identificación, así como una contraseña alfanumérica para su aprobación. Podrán aplicarse configuraciones de complejidad y expiración.

34. El mecanismo de autenticación de usuarios de Targeted Attack Protection es mediante credenciales locales, es decir, consistente en una cuenta de correo electrónico para su identificación, así como una contraseña alfanumérica para su aprobación.

35. Para más información sobre la gestión de contraseñas ver la sección **6.3.2.**

6.3 ADMINISTRACIÓN DEL PRODUCTO

6.3.1 ADMINISTRACIÓN LOCAL Y REMOTA

36. El mecanismo de administración de Email Protection es de forma remota, a través de la interfaz web o webUI. Esta conexión se realiza a través del protocolo https en el puerto 10000 (https://XXXX.pphosted.com:10000/admin, donde XXXX será el identificador de cliente en Proofpoint) y cifrada con un certificado TLS 1.2, usando un cifrado TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 de 256 bits.

37. El mecanismo de administración de Targeted Attack Protection es de forma remota, a través de la interfaz web o webUI. Esta conexión se realiza a través del protocolo https (tcp#443) y cifrada con un certificado TLS 1.2, usando un cifrado TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 de 128 bits.

38. La comunicación con las interfaces web está identificada a través de un certificado digital presentado por Proofpoint, validado por Sectigo y certificado por USERTrust RSA.

39. Esta configuración no es editable.

6.3.2 CONFIGURACIÓN DE ADMINISTRADORES

40. La plataforma de Email Protection permite el establecimiento de distintos usuarios administradores, con atribuciones diferenciadas, si se desea. Esta asignación de atributos y roles o RBAC (Rol Base Access Control) se puede configurar a través del menú Administrators > Roles, seleccionando los módulos sobre los que se les otorga derecho de administración; en el perfil de cada usuario administrador, se podrá asignar el rol deseado.

41. El sistema cuenta con una política predefinida de contraseñas locales, denominada "admin" y accesible a través del menú Administrators > Policy Password. Esta política cuenta con las siguientes características:

    - Permite accesos concurrentes
    - Tiene fecha de expiración a los 90 días, emitiendo alertas 7 días antes
    - La sintaxis consta de entre 12 y 20 caracteres, usando números, símbolos, mayúsculas y minúsculas, y no debe ser igual que el nombre de usuario
    - Ante 3 fallos de introducción errónea de contraseña, de bloquea la IP desde donde se ha realizado 180 segundos, y el usuario 180 segundos

42. Si un usuario administrador necesita un cambio de contraseña, lo puede hacer él mismo, o realizarlo usando el usuario superadministrador inicial de la plataforma denominado podadmin. Este usuario (podadmin) es el único con facultad de poder crear, modificar y eliminar a otros usuarios administradores Si se pierde la contraseña de podadmin, deberá contactar con Soporte de Proofpoint a través del canal de tickets de ayuda, para solicitar una nueva contraseña.

43. Se pueden generar otras políticas de contraseñas o modificar la existente para adecuarse a otros requisitos, pudiéndose modificar los valores antes comentados.

44. A través del menú System > Settings > Admin Server, será posible establecer un tiempo máximo de inactividad de la sesión del usuario administrador. Por defecto este parámetro se establece en 90 minutos, pudiéndose variar su cantidad. Se recomienda establecer un tiempo máximo de 5 minutos.

45. En el mismo menú, se puede activar un mensaje de aviso o disclaimer ante el acceso de un usuario administrador, así como la restricción por direccionamiento IP específico.

6.4 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

46. Proofpoint ofrece la plataforma de Email Protection en formato SaaS (Software as a Service) mantenido con recursos gestionados por Proofpoint y accesible a través de su interfaz web usando el puerto 10000. Se recomienda continuar con esta configuración, pero si se desea, a través del menú System > Settings > Admin Server se puede modificar a otro puerto.

6.5 GESTIÓN DE CERTIFICADOS

47. La plataforma de Proofpoint permite auditar y securizar el flujo de correo de cualquier organización, y por lo tanto, permite aplicar restricciones a la comunicación SMTP.

48. A través del menú System > SMTP Encryption > Settings se puede activar (opción recomendada) del uso de TLS en la comunicación entre gateways de correo, es decir, entre Proofpoint y otros servidores externos mediante SMTP, que en este caso, será sobre TLS. Además, permite seleccionar las versiones del protocolo mínima aceptada, de forma independiente para el tráfico entrante (inbound) y saliente (outbound); se recomienda seleccionar TLS1.2.

49. Si se desea restringir específicamente a los algoritmos de cifrado aprobados por el CCN, se deberá contactar con Soporte de Proofpoint a través del canal de tickets de ayuda, para

solicitar dicha restricción, indicando que se deben eliminar todos los certificados de cifrado excepto los siguientes:

- ECDHE-RSA-AES256-GCM-SHA384 (TLSv1.2)
- ECDHE-RSA-AES128-GCM-SHA256 (TLSv1.2)

50. De esta manera, Email Protection utilizará una negociación restrictiva en la comunicación SMTP sobre TLS, es decir, si se encuentra disponible con el otro extremo (el servidor de correo externo), se negociará la comunicación y se enviará de forma segura.

51. Nota Importante: Si no fuera posible la negociación, ya sea por incompatibilidad de algoritmos de cifrado o incluso la no existencia de TLS en el servidor externo, la seguridad se **rebaja a SMTP en texto plano**. No obstante, se puede configurar el forzado del uso del TLS seleccionado en Proofpoint en la comunicación. En el menú System > Email Encryption > TLS Domains se pueden incluir direcciones IP o dominios concretos, a los que exigir siempre la comunicación sobre TLS. Esta configuración sólo se recomienda activar con los dominios de probada existencia de una comunicación cifrada, para evitar pérdida de mensajes.

6.6 SERVIDORES DE AUTENTICACIÓN

52. La plataforma de Email Protection y Targeted Attack Protection utilizan servidores de autenticación internos por defecto, por lo que no se necesita realizar ninguna configuración adicional.

6.7 SINCRONIZACIÓN

53. Proofpoint ofrece la plataforma de Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, por lo que la gestión de la sincronización horaria del producto es realizada por Proofpoint, sin que el usuario administrador deba realizar ninguna acción.

6.8 ACTUALIZACIONES

54. La plataforma Email Protection dispone de una configuración de aplicación de actualizaciones de forma automática tan pronto como están disponibles, si necesidad de realizar ninguna acción adicional. Esta es la configuración adecuada y recomendada.

55. No obstante, se puede comprobar a través del menú System > Licenses and Updates, pudiéndose decidir realizar la instalación de las actualizaciones en el sistema de filtrado, en franjas horarias seleccionadas de mantenimiento.

6.9 AUTO-CHEQUEOS

56. Proofpoint ofrece la plataforma de Email Protection y Targeted Attack Protection en formato SaaS (Software as a Service) mantenido con recursos gestionados por Proofpoint, por lo que la gestión de autocomprobaciones se realiza de forma interna, sin que el usuario administrador deba realizar ninguna acción.

6.10 ALTA DISPONIBILIDAD

57. Proofpoint ofrece la plataforma de Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, manteniendo los más altos estándares de redundancia, protección y alta disponibilidad, así como recuperación ante desastres forma interna, sin que el usuario administrador deba realizar ninguna acción.

6.11 AUDITORÍA

6.11.1 REGISTRO DE EVENTOS

58. La plataforma de Email Protection permite la visualización de registro de eventos de auditoría (realizados por usuarios administradores y el propio sistema) a través del menú Logs and Reports > Audit Logs. Cada entrada dispone un detalle de la fecha del evento, la dirección IP desde donde está hecha la conexión, el usuario, y la acción.

59. Esto es un ejemplo:

Date	Access From	Administrator	Activity
2024-01-31 20:57:08 [UTC+0100]	84.15.180.154	xxxx	Login

Tabla 1: Ejemplo de log de evento

60. Además, se dispone el detalle de los registros de auditoría de la configuración, contando con los siguientes campos:

- **Date:** Fecha/hora (*timestamp*) de la modificación.
- **Modified By:** Usuario que realiza la modificación.
- **Before Modification:** Estado antes de la modificación.
- **After Modification:** Estado tras la modificación.

61. A continuación, se pueden ver dos ejemplos:

Date	Modified By	Before Modification	After Modification
2024-01-31 20:57:08 [UTC+0100]	xxxx@mxxxx.ppops.net	empty	com.proofpoint.filter.module.access.rule.03_ emisores_internos_block.comments.1503=
2024-01-31 19:45:14 [UTC+0100]	xxxx@mxxxx.ppops.net	com.proofpoint.filter.module.access.rule.03 _emisores_internos_block.conditions=||,9,50,53,54,64,94	com.proofpoint.filter.module.access.rule.03_ emisores_internos_block.conditions=||,9,50,53,54,64,94,154,200,221

Tabla 2: Ejemplo de log de evento de configuración

6.11.2 ALMACENAMIENTO

62. Proofpoint ofrece la plataforma de Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, y toda actividad de almacenamiento de registros de eventos, se almacenan en la propia base de datos del sistema, protegido de forma automática con cifrado AES-256.

63. Su gestión se realiza de forma automática por Proofpoint, sin que el usuario administrador deba realizar ninguna acción.

6.12 BACKUP

64. Proofpoint ofrece la plataforma de Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, manteniendo los más altos estándares de resiliencia, por lo que realiza de forma periódica (una vez al día en horario nocturno) una copia de seguridad de la configuración del sistema y almacenándolo de forma externa y cifrada, con un guardado de los últimos 14 *backups*, sin que el usuario administrador deba realizar ninguna acción.

65. Estos *backups* son sólo utilizables por Proofpoint en caso de necesidad.

7 FASE DE OPERACIÓN

66. Proofpoint ofrece la plataforma de Email Protection y Targeted Attack Protection en formato SaaS (*Software as a Service*) mantenido con recursos gestionados por Proofpoint, realizándose la supervisión del buen funcionamiento del sistema por Proofpoint, sin que el usuario administrador deba realizar ninguna acción.

67. Se podrá observar en el registro de mensajes procesados, un sistema de monitorización de procesado de correo de Proofpoint. Consiste en el envío de mensajes a través de la plataforma y salida al siguiente salto, para verificar que el sistema funciona correctamente. Se puede observar esta situación en Smart Search y no es necesario realizar ninguna acción adicional por parte de un administrador, ya que está supervisado por Proofpoint.

Date	2024-01-31 20:57:08 [UTC+0100]
Sender	mailive@knowledgefront.com
Recipients	mailive@knowledgefront.com
Subject	Mailive! Test - [FSMAILID:gmExdGNtdHF1bG84dWpzMWNxdXVqMjFn]
Final Action	Sent

Tabla 3: Ejemplo de información de Smart Search

68. Se recomienda a un usuario administrador, la personalización de las alertas del sistema, para que se reciban a través de un correo cuando se desencadene alguna situación supervisada de interés. Para realizarlo, pueden acceder al menú System > Alerts > Alerts Profiles y generar un nuevo perfil con el botón “Add” para incluir un/os destinatarios. A continuación, en System > Alerts > Rules se podrá añadir una nueva regla con el botón “Add” y seleccionar las condiciones de la alerta; se recomienda utilizar al menos:

- *General error.*
- *Cannot connect to update server.*
- *Running out of disk space.*
- *Deploy failed.*
- *Update available.*
- *Patch applied & reboot is required.*
- *Upgrade failed.*
- *User repository import alert.*
- *SMTP queue above threshold.*
- *License will expire.*
- *License expired.*
- *Folder injection rate reset.*
- *Folder injection rate alert.*
- *Appliance hardware alert*.

69. De forma complementaria, Proofpoint dispone de una supervisión activa sobre la plataforma, por lo que Proofpoint puede lanzar tareas de mantenimiento y/o corrección ante una situación no deseada de forma proactiva. Estas actividades están bajo la responsabilidad de Proofpoint y son debidamente notificadas a los administradores.

8 REFERENCIAS

REF1 Proofpoint on Demand (PoD) Administration Guide – Release 8.18.X

9 ABREVIATURAS

BEC	Business Email Compromise
DKIM	DomainKeys Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL
MLX	Machine Learning eXperience
RBAC	Role-Based Access Control
SaaS	Software as a Service
SCSS	Stateful Composite Scoring Service
SPF	Sender Policy Framework
SMTP	Simple Mail Transfer Protocol
TAP	Targeted Attack Protection
TLS	Transport Layer Security
URL	Uniform Resource Locator
VIP	Virtual IP
ENS	Esquema Nacional de Seguridad.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL