centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1463

Procedimiento de Empleo Seguro
Symantec Web Protection Suite

Diciembre 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: 083-24-315-5.
Fecha de Edición: diciembre de 2024

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
2024.12.23 18:11:38 +01'00'

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. Symantec Web Protection Suite es una solución proxy, que se encuentra desplegada en la nube, que proporciona una amplia gama de herramientas diseñadas para proteger a las organizaciones contra amenazas en línea y para ayudar a administrar el acceso a Internet de manera segura. Algunas de las características comunes de las soluciones de protección web incluyen:

   a) Filtrado de contenido web: controla y monitorea el acceso a sitios web basándose en categorías predefinidas, políticas personalizadas o listas negras y blancas.

   b) Protección contra malware y amenazas en la web: identifica y bloquea activamente sitios web maliciosos, URLs sospechosas y ataques basados en la web, como phishing y descargas de malware.

   c) Seguridad de datos: ayuda a prevenir la fuga de datos al monitorear y controlar las transferencias de datos sensibles a través de la web, aplicando políticas de seguridad y cifrado si es necesario.

   d) Análisis de tráfico web: proporciona visibilidad y análisis detallados sobre el tráfico web para identificar patrones de uso, tendencias de amenazas y posibles problemas de seguridad.

   e) Control de aplicaciones: gestiona el acceso a aplicaciones web específicas, controlando qué aplicaciones pueden ser utilizadas y qué acciones pueden realizar los usuarios.

2. La solución de Web Protection Symantec es una solución integral que puede ayudar a las organizaciones a mantenerse seguras mientras navegan por la web y utilizan recursos en línea.

2 OBJETO Y ALCANCE

3. En la presente guía se recoge el procedimiento de empleo seguro para la plataforma Symantec Web Protection Suite. Para ello, se ha basado en la información publicada para la administración de la plataforma [REF1].
4. El servicio Symantec Web Protection Suite ha sido **cualificado** en el catálogo CPSTIC para **categoría ENS MEDIA en la familia Proxies.**
5. El Symantec Web Protection es un Proxy, que se encarga de la protección de las interconexiones, siendo el intermediario cuando se produce un intercambio de peticiones entre usuarios de una red y recursos ubicados en una red diferente. Symantec Web Protection es un servicio de seguridad que proporciona seguridad avanzada de datos, aplicaciones y usuarios, independientemente de su ubicación. Para ello, dispone de una consola desde la que un administrador de la organización puede crear políticas y observar las comunicaciones de los usuarios.
6. Por otro lado, los usuarios requieren la instalación de un fichero que se encarga de enrutar las comunicaciones a través de Symantec Web Protection. El alcance está compuesto por la consola Cloud Web Security, que se encuentra en la nube, y los equipos a monitorizar
7. Como se ha mencionado anteriormente, estos componentes se definen de la siguiente manera:

    - **Cloud Web Security**, es la consola alojada en la nube que se encarga de la configuración del proxy para los distintos usuarios finales que la utilizan. La consola está alojada en Google Cloud Platform. Proporciona una visión general de las páginas web y aplicaciones a las que acceden los usuarios, actividad de los usuarios y páginas bloqueadas. Cloud Security Service se encarga de proporcionar al administrador la siguiente información:
        - Dashboard donde se puede observar la actividad de los Agentes WSS
        - Informes
        - Opción de descarga del Agente WSS y su preconfiguración
        - Políticas para cada uno de los endpoints
        - La configuración del propio Cloud Security Service
    - **Fichero PAC**, es el software instalado en los endpoints de los usuarios. Se encarga de enviar a Cloud Web Security la siguiente información:
        - la actividad del usuario final
        - cómo enruta el tráfico, Además, el Agente WSS se comunica con la consola para la sincronización de las políticas que se implementan en la consola.

3 ORGANIZACIÓN DEL DOCUMENTO

8. El presente documento se divide en las siguientes partes fundamentales, de acuerdo con distintas fases que componen el ciclo de vida del producto:

   a) Apartado **4**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.

   b) Apartado **5**. En este apartado se recogen las recomendaciones a tener en cuenta durante la fase de configuración del producto, para lograr una configuración segura.

4 FASE PREVIA A LA INSTALACIÓN

4.1 ACTIVACION DEL PRODUCTO

9. Para comenzar a utilizar la solución de Web protection Suite (WPS) y sus otros servicios en la nube de Symantec hay que registrarse en el Portal Cloud Management (CMP). Es un portal centralizado para ver el estado y la configuración de sus suscripciones a la nube de Symantec. Cuando adquiera suscripciones básicas de Cloud SWG o productos complementarios de Cloud SWG, recibirá un mensaje de correo electrónico de Broadcom que incluye un enlace al CMP para configurar las suscripciones.
10. Para acceder al CMP por primera vez y configurar los servicios en la nube, completa los siguientes pasos:
    a) Cree una cuenta segura para iniciar sesión en el CMP. El enlace es https://cmp.protect.broadcom.com
    b) Busque el correo electrónico de Broadcom en su bandeja de entrada. Si no lo encuentra en la bandeja de entrada, compruebe la carpeta de correo no deseado. Haga clic en el enlace de este correo electrónico para crear su cuenta de inicio de sesión segura. Si usted no es el usuario registrado al que se envió el correo electrónico, póngase en contacto con un usuario registrado de su empresa. Cualquier usuario registrado puede añadirle a su cuenta corporativa como usuario registrado.
    c) Utilizando la cuenta que creó en el paso anterior, inicie sesión en el CMP.
    d) El CMP muestra los servicios en la nube que ha adquirido. Puede configurarlos para su configuración particular de reenvío de correo electrónico.
    e) Después de configurar y revisar sus servicios en la nube de Symantec en CMP, puede iniciar sesión en el portal de Web Protection Suite. El acceso a este portal se realiza en el siguiente enlace: Web Security Service
11. Cuando accede al portal de SWG Nube por primera vez, el navegador muestra la primera página del Asistente de configuración inicial. En este paso, es necesario definir las credenciales de administrador y establecer una plantilla de política predeterminada inicial. Puede realizar todas las configuraciones de conexión y definiciones de políticas personalizadas más adelante.

4.2 REQUISITOS TECNICOS

12. La mayoría de los métodos de conectividad y autenticación de Cloud SWG requieren comunicación a través de puertos, protocolos y servicios específicos. Compruebe que los puertos y servicios que utiliza están abiertos en su cortafuegos. Estos requisitos son
13. Para los agentes hay que permitir los siguientes puertos:

DIRECCION/URL	PUERTO	MOTIVO
ctc.threatpulse.com 130.211.30.2	TCP 443	Controlador primario de tráfico en la nube (CTC), que proporciona enrutamiento y configuraciones de agentes a los agentes.

DIRECCION/URL	PUERTO	MOTIVO
ctc-uat.threatpulse.com 34.110.245.218	TCP 443	CTC secundario, que proporciona enrutamiento y configuraciones a los agentes
Listado de Data Centers en KB 167174	TCP 80 TCP/UDP 443	Conexiones de agentes a métodos de conectividad de ubicación fija

Tabla 1. Puertos de agentes

14. Para la autenticación hay que permitir los siguientes puertos:

    a) Para la conectividad del componente Auth Connector hay que permitir los siguientes puertos:

DIRECCION/URL	PUERTO	MOTIVO
Auth Connector server	TCP 80	Conectividad entre clientes que ejecutan ACLogon.exe y el servidor Auth Connector
auth.threatpulse.com 34.160.229.36	TCP 443	Auth Connector Conexion con WPS
proxy.threatpulse.net Este nombre resuelve el portal de WPS	TCP 8080	Roaming Captive
saml.threatpulse.net 199.19.248.205	TCP 8443 (over VPN)	Redirección SAML para el proxy explícito e IPSec

Tabla 2. Puertos del Auth Connector

    b) Para la integración de grupos y usuarios del Directorio Activo hay que permitir los siguientes puertos:

PROTOCOLO	PUERTO
ADSI LDAP	TCP 3268
Kerberos	TCP 88
LDAP	TCP 389
Location Services/RPC	TCP 135
SMB	TCP 139 TCP 445
SSL/TLS	TCP 443

Tabla 3. Puertos del Directorio Activo

15. Dependiendo del método de conectividad

a) Para el plugin de Chrome hay que permitir los siguientes puertos:

DIRECCION/URL	PROTOCOLO	PUERTO	MOTIVO
Dispositivo compatible con el navegador Chrome	HTTP/2	TCP 8080	Proteger el tráfico web desde el dispositivo y admitir la autenticación a través del portal cautivo itinerante.

Tabla 4. Puertos del plugin de Chrome

b) Para el proxy explicito hay que permitir los siguientes puertos:

DIRECCION/URL	PROTOCOLO	PUERTO	MOTIVO
pfms.wss.symantec.com 34.120.17.44	HTTPS	TCP 443	Explicit Proxy PAC File Management System (PFMS)
portal.threatpulse.com/pac	HTTP	TCP 8080	Permite a WPS usar el Pac F

Tabla 5. Puertos del Proxy explicito

c) Para el proxy explícito sobre IPSec hay que permitir los siguientes puertos:

DIRECCION/URL	PROTOCOLO	PUERTO	MOTIVO
ep.threatpulse.net 199.19.250.205 ep-roundrobin.threatpulse.net ep-all.threatpulse.net 199.19.248.205 199.19.250.205 199.19.250.206 199.19.250.207 199.19.250.208 199.19.250.209 199.19.250.210 199.19.250.211 199.19.250.212 199.19.250.213 199.19.250.214 Estas direcciones estan en el tunel IPSec	IPSec/ESP	UDP 500 (ISAKMP) UDP 4500 si el firewall esta detras del NAT	Cloud proxy services

Tabla 6. Puertos del Proxy explícito sobre IPSec

d) Para IPSec hay que permitir los siguientes puertos:

PROTOCOLO	PUERTO	MOTIVO
IPSec/ESP	UDP 500 (ISAKMP) UDP 4500 si el cortafuego este detrás del NAT	Establecer el tunel de VPN seguro

Tabla 7. Puertos IPSec

e) Para el proxy Forwarding hay que permitir los siguientes puertos:

DIRECCION/URL	PROTOCOLO	PUERTO	MOTIVO
proxy.threatpulse.net	HTTP	TCP 8080	Reenvía el tráfico a los hosts del dispositivo SWG Edge
	HTTPS	TCP 8443	
	HTTPS	TCP 8084	Reenvío de tráfico a hosts configurados para la interceptación SSL local en el dispositivo SWG Edge

Tabla 8. Puertos del Proxy Forwarding

f) Para permitir el acceso a los portales Portales hay que permitir los siguientes puertos:

DIRECCION/URL	PROTOCOLO	PUERTO	MOTIVO
portal.threatpulse.com 34.49.9.67	HTTPS	TCP 443	Descargas del agente de administración de WPS en la nube Descargas de Auth Connector.
support.broadcom.com	HTTPS	TCP 443	Base de datos de artículos de soporte.

Tabla 9. Puertos de los portales

4.3 REGISTRO Y LICENCIAS

16. Antes de iniciar el proceso de registro, complete los siguientes pasos para activar la licencia:
    a) Recibirá un correo de bienvenida a la hora de realizar la adquisición del producto donde estará ID de suscripción de la solución.
    b) A la hora de la compra de licencia, tendrá que facilitar una dirección de correo electrónico para asociarla a la cuenta del portal SWG de Nube.
    c) Cloud SWG utiliza el proveedor de identidades (IdP) Okta para autorizar el acceso al administrador.
17. Para complementar el registro hay que acceder a la siguiente URL. https://portal.threatpulse.com/register
18. A continuación, se crea un administrador:

a) Introduzca la dirección de correo electrónico y el nombre del administrador principal de Cloud SWG, es decir, el que se facilitó durante el proceso de compra.

b) Introduzca el ID de suscripción que se encuentra en el correo de bienvenida.

c) Certifique que ha leído el EULA

d) Hacer click en Registrar

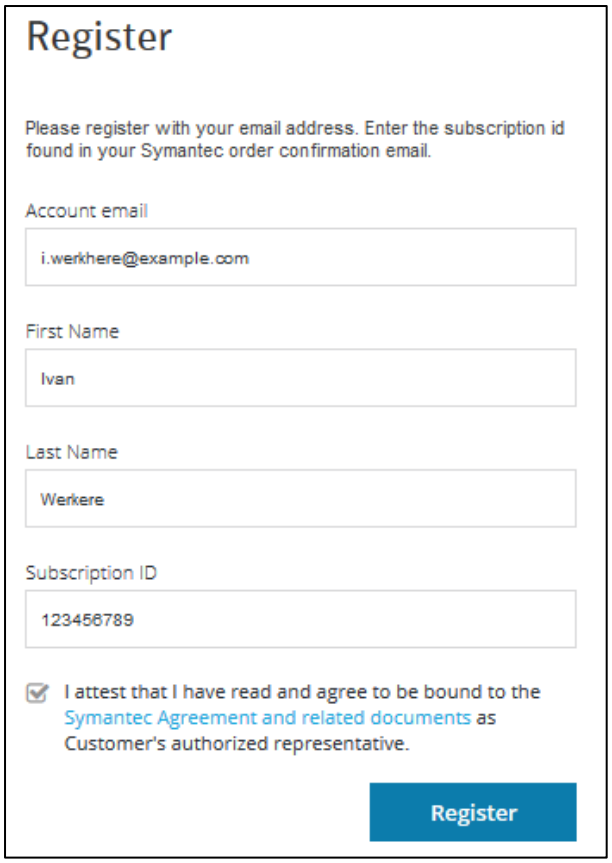

Ilustración 1. Registro de licencia ID

e) El portal muestra un cuadro de diálogo en el que se le informa de que debe comprobar la cuenta de correo electrónico recién registrada.

f) En ese correo electrónico, copie la contraseña temporal.

g) Cierra el diálogo.

19. Una vez creado el administrador, se da por finalizado el registro de las licencias.

5 FASE DE CONFIGURACIÓN

5.1 AUTENTICACIÓN DE ADMINISTRADORES

20. Tras haber realizado el registro de las licencias, comienza la fase de configuración de la solución. El primer paso es la creación de los usuarios administradores de la plataforma. Por defecto, WPS usa el IdP de Okta para identificar a los administradores.

21. Con el correo de administrador y la contraseña temporal acceda al portal. La primera vez que acceda, la solución le pedirá cambiar la contraseña temporal. Además, si su empresa requiere autenticación de múltiples factores (MFA), se le pedirá que complete esta configuración.

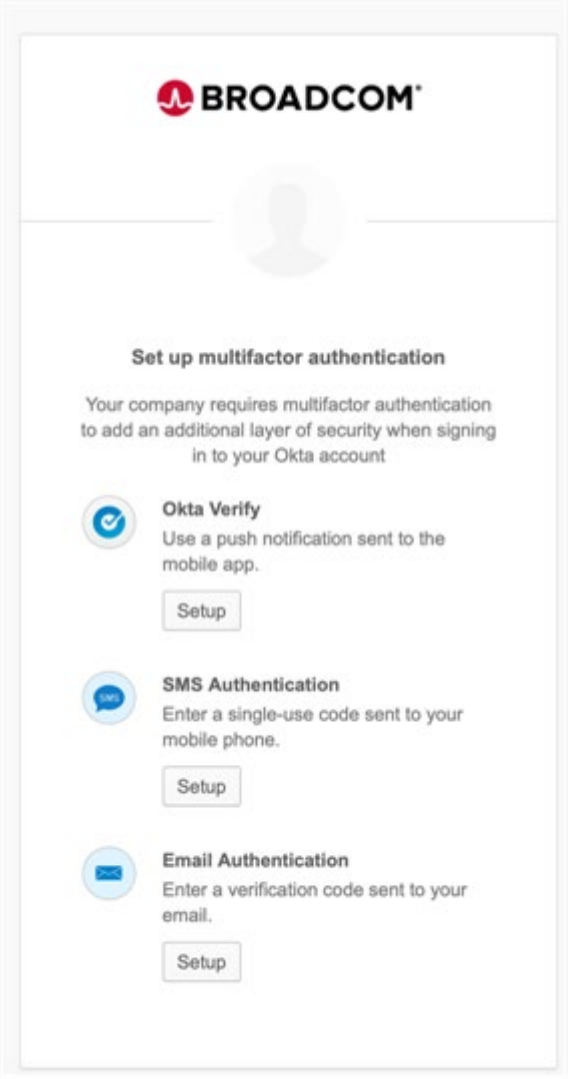

Ilustración 2. Configuración MFA

22. Cloud SWG comienza la segunda fase de configuración inicial, la primera de las cuales es la Configuración del producto.

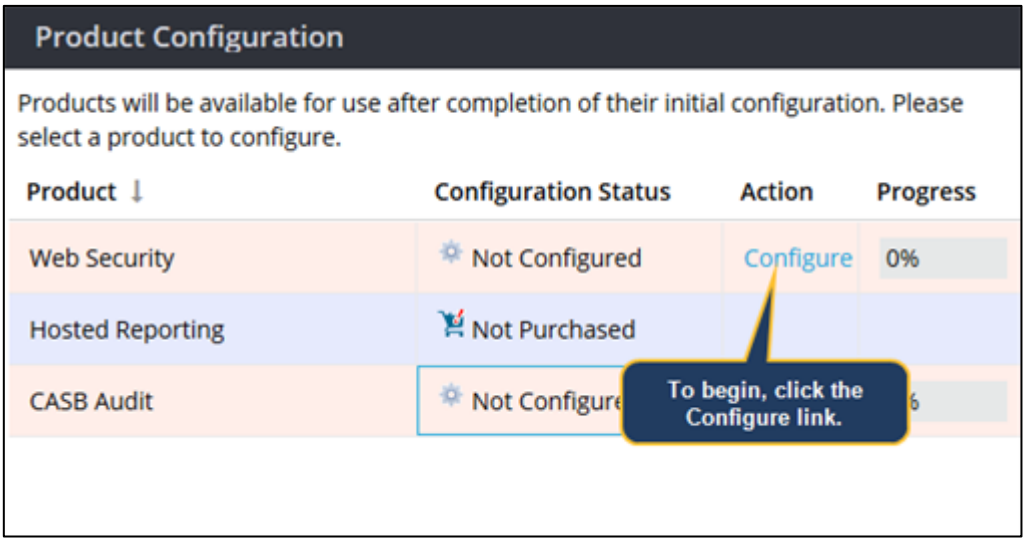

Ilustración 3. Configuración del producto

23. Configuración de los parámetros de sesión. El tiempo de espera de la sesión del portal SWG está establecido en 15 minutos. Este valor no se puede modificar

24. Sobre la política de contraseña, al tener como proveedor de identidad de los usuarios a Okta, usa las políticas de esta solución. En este proveedor podemos configurar políticas como:

    a) Mínima longitud

    b) Complejidad de la contraseña

    c) Chequeo de contraseñas comunes

    d) Antigüedad de la contraseña

25. Para más información sobre la política de configuración de contraseñas hay que acudir a la documentación de Okta sobre políticas de contraseñas [REF3].

5.1.1 CONFIGURACIÓN DE ADMINISTRADORES

26. Para una mayor seguridad, asegúrese de que se permite un acceso mínimo al portal WPS. Gestione los roles de los usuarios y otros ajustes de la cuenta para restringir el nivel de acceso y el tiempo durante el cual el acceso es válido. Como usuario administrador, puede editar los ajustes de su propio perfil y gestionar el acceso y los roles de otros usuarios administradores. Por ejemplo, puede cambiar el rol predeterminado o desactivar temporalmente el acceso del usuario.

27. Para la creación de administradores, hay que seguir los siguentes pasos:

    a) En el portal de SWG en la nube, seleccione Configuración de cuenta ->Administradores.

    b) Hacer click en añadir cliente usuario

    c) Indica el nombre y apellidos del administrador

    d) Introduzca el correo del administrador. WPS se encargará de llegarle un correo con las credenciales para acceder.

e) Seleccione un rol para este administrador.

f) Guarde y el administrador se añadirá a la solución

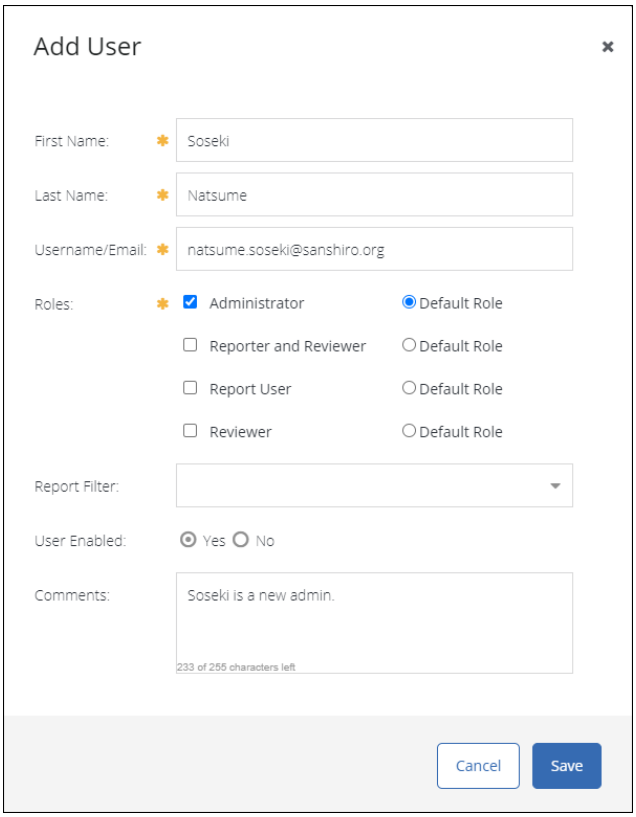

Ilustración 4. Guardado del administrador

5.1.2 ROLES

28. Como administrador de SWG Nube, puede conceder a cada administrador un acceso al portal con distintos privilegios basados en las funciones de los usuarios de la organización. Existen unos roles ya predefinidos en la consola o se puede crear uno manualmente.

29. Entre los roles predefinidos encontramos los siguientes:

    a) **Administrador**: El rol de Administrador proporciona acceso completo a todas las páginas y configuraciones del portal. Un Administrador puede configurar la provisión de cuentas de usuario, los métodos de conectividad de tráfico, las políticas y la generación de informes.

    b) **Report User**. El rol de report user proporciona acceso completo a los informes y ningún acceso a las configuraciones de servicio. Por ejemplo, asigne este rol a un empleado de Recursos Humanos que deba realizar un seguimiento del uso de Internet de los empleados de un grupo específico. Cree un filtro por ubicación, subred u otros criterios. Puede limitar el tipo de datos que se muestran en los informes. Por ejemplo, si al empleado de Recursos Humanos no le interesan los valores de puerto o dirección IP del cliente, elimine esos campos del rol.

    c) **Reviewer**. El rol de Revisor otorga acceso de sólo lectura a algunas áreas. Los usuarios no pueden añadir o cambiar ninguna configuración, y algunas páginas están ocultas.

Por ejemplo, asigne esta función a un consultor de seguridad externo que necesite acceder a las políticas de auditoría.

d) **Reporter-Reviewer**. El rol Reporter-Reviewer combina los permisos del Usuario de Informes y del Revisor. De este modo, el Reportero-Revisor tiene acceso total a los informes y acceso de sólo lectura a algunas áreas de WPS.

5.2 CONECTIVIDAD DE LOS USUARIOS

30. Para redirigir el tráfico de los usuarios a la plataforma Symantec Web Protection existen varias formas de hacerlo posible de los componentes que se quieran usar.

    a) Por localización El estado de conexión de las ubicaciones fijas. Dentro de este modo existe:

    - Virtual Private Network (IPsec)
    - Proxy Forwarding
    - Explicit Proxy

    b) Agentes. La conectividad la realiza agentes instalado en los equipos (WSS agente, SEP, SEP Mobile)

31. Dependiendo de las necesidades y condiciones de cada organización se decidirá una u otra siguiendo los procedimientos definidos en [REF4].

32. Proxy explicito es una solución muy común en el mercado, pero como se ha comentado, se puede utilizar otra de las disponibles.

33. Proxy explícito se refiere al método de utilizar la configuración local de los navegadores de los clientes para dirigir el tráfico a servidores proxy que alojan archivos PAC. Un archivo PAC es un fichero JavaScript que automatiza a través de qué proxies se comunican los navegadores web para llegar a Internet.

34. Estos ficheros PAC puede ser gestionados por el sistema de gestión de archivos PAC (PFMS) de WPS que se encuentra dentro de la solución. Gracias a este servicio se puede crear y administrar estos ficheros PAC de forma flexible, dependiendo de las necesidades del cliente.

35. Por ejemplo, desea que los equipos de trabajo que trabajan desde una localización utilicen un fichero PAC que, por ejemplo, omita servidores específicos y solicitudes de Office 365 o que no conecte con el servicio de WPS y vaya directamente al proxy on-premise. Sin embargo, si estos equipos trabajan de forma remota, se le puede aplicar otro fichero PAC que redirija el tráfico a la solución de WPS siempre se conectan.

5.2.1 COMUNICACIONES SEGURAS

36. Existe una posible configuración que se puede realizar para seguir las recomendaciones que sugiere ENS. Esta configuración hace referencia al documento CCN-STIC-807 [REF2] que se basa en los mecanismos criptográficos que emplea el producto para cifrar las comunicaciones entre la consola y los agentes.

37. Lo que aconseja en la guía de seguridad es limitar estos mecanismos para solo usar los que se consideren seguros. Por ejemplo, TLSv1.2 o TLSv1.3 o el uso de claves de cifrados y curvas elípticas para el cifrado.

38. Para poder limitar todo ello, existe un proceso para limitar el uso de claves de cifrado o TLS y es a través de soporte. **El administrador de las licencias tiene que abrir un caso con soporte e indicar que protocolo o claves de cifrados quiere usar y restringir el resto.**

5.3 SERVIDORES DE AUTENTICACIÓN

39. Para la identificación de los usuarios, WPS soporta varios protocolos, entre ellos SAML. Es el más extendido en el mercado y por ello se ha usado este protocolo como el estándar. WPS es compatible con este método y permite la gestión de usuario con una implementación SAML ya existente en la organización. Existe integración con los siguientes sistemas de IdP:

    a) Microsoft AD Azure

    b) Google WorkSpace

    c) Okta

    d) Ping Identity

    e) Symantec VIP Access

    f) SAML IdP

40. Para todos estos métodos, se necesita una serie de información que se debe de exportar de la consola de gestión WPS al IdP. Esta información se encuentra dentro de la consola en Identity > SAML Authentication. Dentro de este apartado se selecciona que IdP se ha decidido usar y la información siguiente:

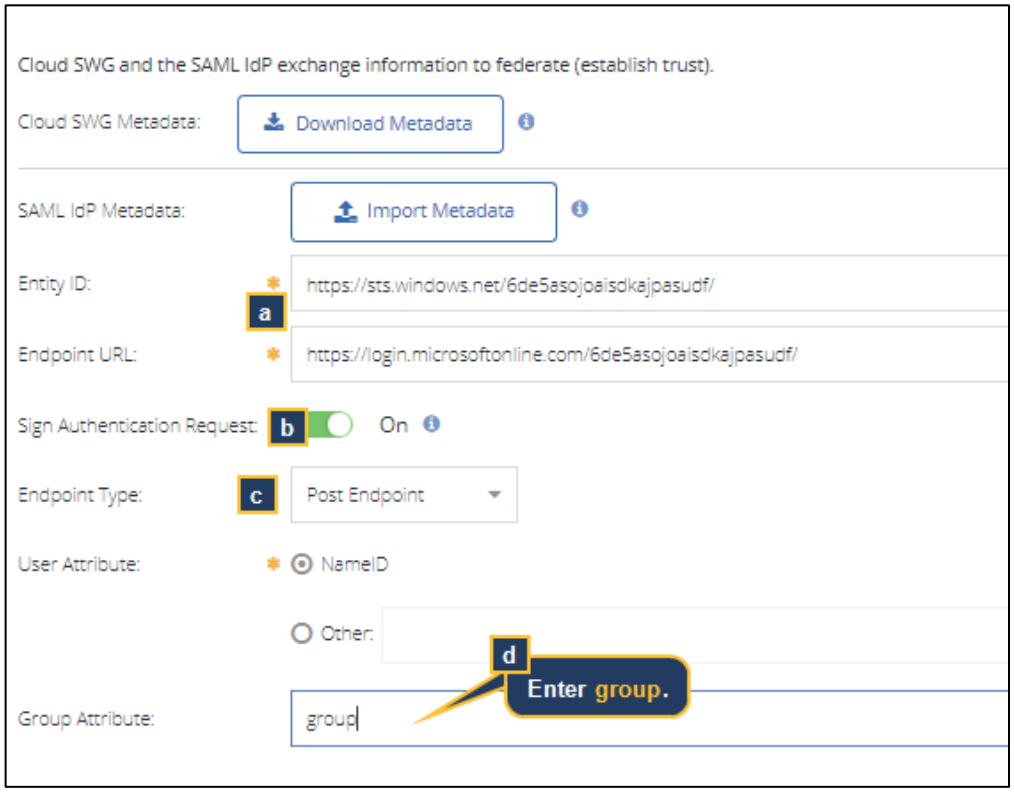

Ilustración 5. Informacion IdP

a) Entity ID y endpoint URL si es necesario

b) Que se necesite la identidad del usuario o no

c) Tipo de conectividad que va a tener

d) Atributo que se usara para dividir a los usuarios

5.3.1 INTEGRACION CON GOOGLE WORKSPACE

41. Como prueba de como se hace, se va a realizar un ejemplo de implementación con el servicio de Google se necesita los siguientes requisitos:

    a) Una cuenta de Google G Suite

    b) Un nombre de dominio

42. Otro requisito seria añadir la URL “accounts.google.com” en las excepciones de autenticación

43. Una vez se obtiene estos requisitos, habrá que registrar el dominio en el sistema de Google G Suite. Para más información, acudir a la información proporcionada por Google.

44. Para la integración de la arquitectura SAML y WPS, hay que identificarse en la consola de administración de G Suite “https://admin.google.com”.

45. Accede a SAML y a continuación haga clic en el icono “+” situado en la parte inferior derecha de la página. La interfaz muestra “ActivarSSO para app SAML”

46. Aparecerá un listado de aplicaciones. Entre todas ellas, localiza una llamada SymantecWSS

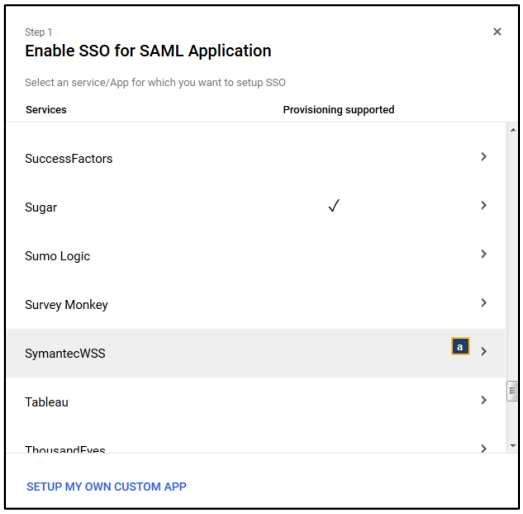

Ilustración 6. Localización de SymantecWSS

47. Haga clic en la flecha de la derecha de SymantecWSS

48. El interfaz muestra el dialogo de Google IdP.

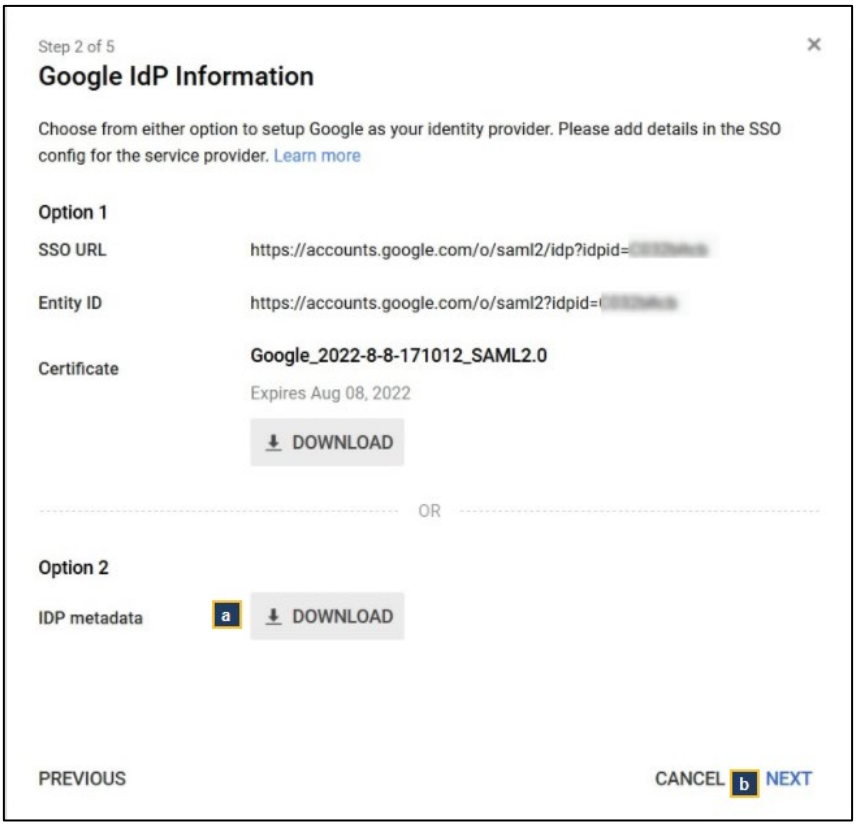

Ilustración 7. Dialogo de Gooble IdP

49. Hay que descargar y guardar el fichero de la opción 2, el fichero de Google IdP. Este archivo se utilizará luego para completar la integración entre el portar de WPS y Google
50. Clic en “Next”.
51. Confirma la información básica sobre la nueva app de SAML. Debería de mostrar la misma información que se muestra en la siguiente imagen:

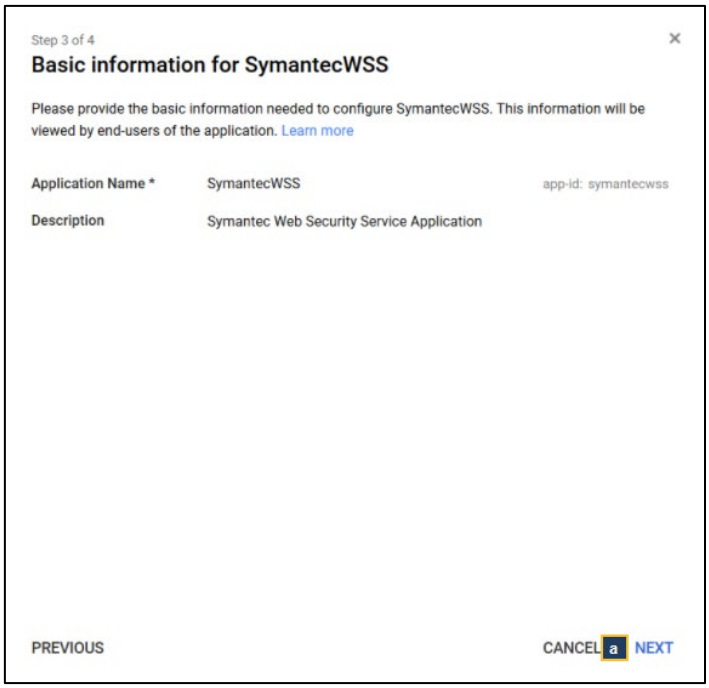

Ilustración 8. Información básica de SAML

52. Clic en “Next”.
53. Se define los parámetros necesarios para la correcta integración:
    a) ACS URL: threatpulse.net:8443/saml/saml_realm/bcsamlpost
    b) Entity ID: https://saml.threatpulse.net:8443/saml/saml_realm
    c) Los demás parametros se pueden dejar en los valores por defecto.
    d) Clic en “Next”

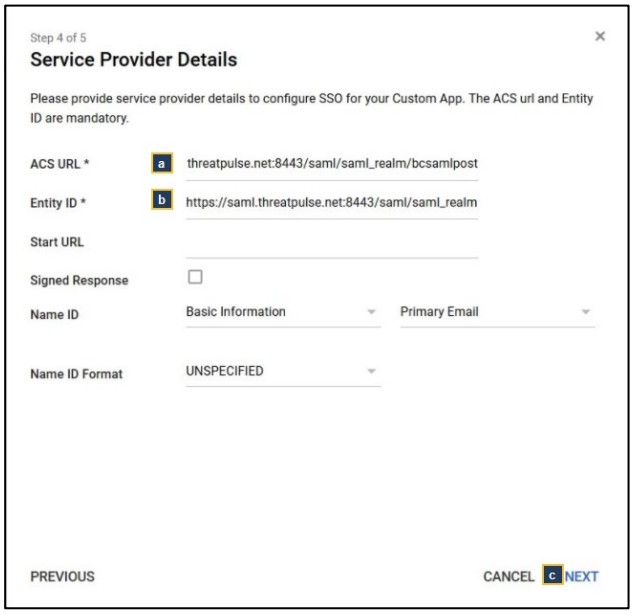

Ilustración 9. Detalles del Service Provider

54. Se define los identificadores de los usuarios y grupos. Las definiciones de grupo que puedan existir actualmente en su configuración de WPS no se pueden importar al servicio de autenticación de G Suite. Esta página le permite asignar atributos de grupo al grupo Departamento.

55. Haga clic en Agregar nueva asignación para utilizar el campo Departamento como grupo de usuarios. Los grupos definidos aquí como Departamentos se pueden utilizar en la política de grupo WPS. Debería queda como muestra la siguiente imagen:

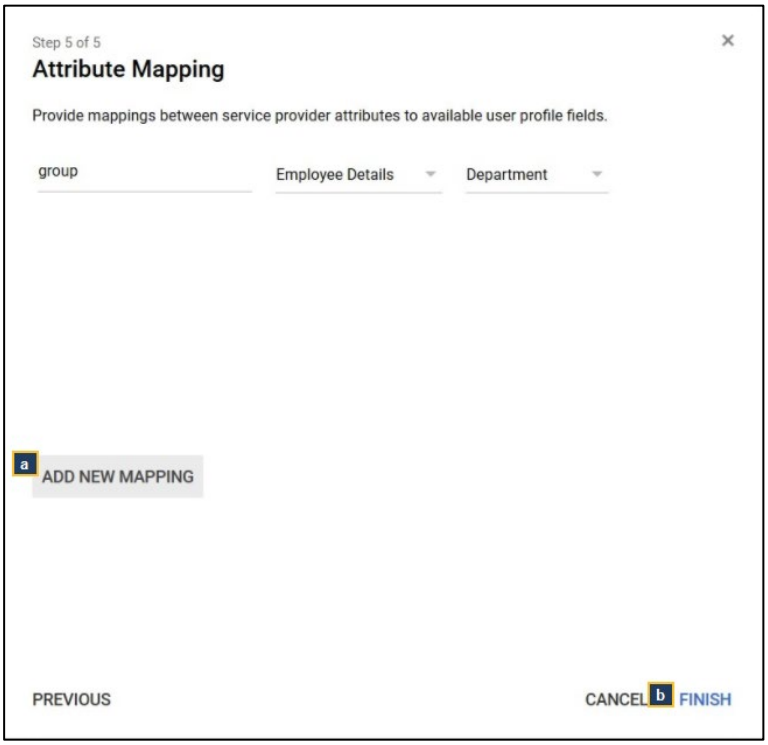

Ilustración 10. Definición de grupos

56. Clic en “Finish”.

57. Después de completar el asistente de configuración de la aplicación G Suite, G Suite muestra una página de configuración.

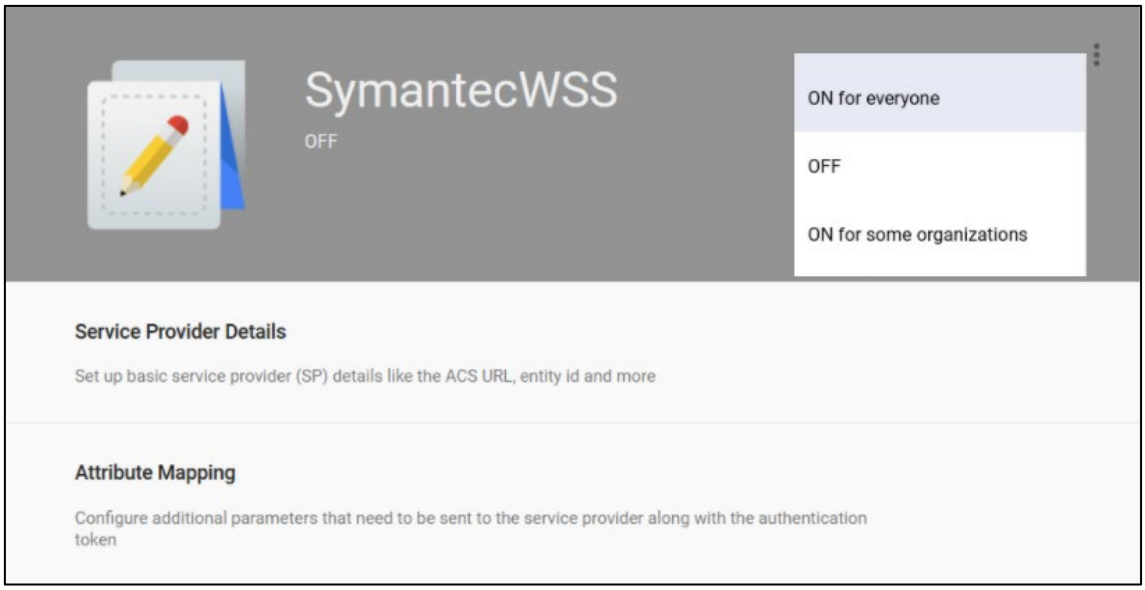

Ilustración 11. Página de configuración

58. Haga clic en el menú de tres puntos de la parte superior derecha y seleccione Activado para todos para activar la autenticación SAML para todos los usuarios.
59. Ahora hay que registrar la integración en el portal de WPS.
60. Accede al portal de WPS y navegue en Identity->SAML Authentication.
61. Expende la información de SAML.
    a) Haga clic en SAML IdP Metadata: Imprt. Busque el archivo de certificado Gsuite guardado en el paso anterior y ábralo. El portal rellena los campos Entity ID, Endpoint URL y Signing Certificate.
    b) Seleccione “Sign Authentication Request” para que el servicio de WPS firme las solicitudes SAML que se envían al IdP. El IdP para validar quién realiza la solicitud de autenticación. Al descargarlo, el archivo de metadatos de WSS contiene el certificado necesario. Este paso es opcional.
    c) Los metadatos importados también incluyen el tipo de agente que se use:
        - Opción de redireccionamiento de la solicitud del endpoint. Es la opción más sencilla y la usada en este documento.
        - Si ha seleccionado la opción Sign Authentication Request, seleccione Post Endpoint (AuthResponses).
    d) En el campo de “Group Attribute”, añadir “group”.
    e) Clic en guardar.
62. Para validar que toda la configuración ha sido correcta, se puede realizar una prueba. Consiste en indicar un proxy explicito en el navegador de un equipo hacia WPS.
63. Para realizar esta prueba, accede al portal de WPS. Añade una localización (Connectivity > Locations). Indicar un nombre, como puede ser “SAML Google Test”. Indique que es “Explicit Proxy” y guarde.

64. Navegue a Identity > Authenticaton Policy. Cree una regla y selecciona “Explicity Proxy Locations”. Se le mostrara una interfaz para esta nueva regla. Clic en “Add Sources” y añada “Explicy Proxy Location”
65. En “Veredict”, permita “Captive Portal” y seleccione SAML. Añada la regla y actívela.
66. Una vez realizados estos pasos, acceda al equipo de pruebas y abra el navegador. Configure el proxy como “proxy.threatpulse.net:8080”. Con este, reinicie el navegador y al volver a acceder, le pedirá que se autentique en Google G Suite para acceder a la navegación.

5.4 CONFIGURACION DE POLITICAS

67. Una vez configurado la redirección del tráfico de los usuarios autenticados hacia la plataforma de WPS, es importante establecer los parámetros de seguridad de navegación y tráfico de red que van a tener los usuarios. Las políticas aplicadas en el portal de WPS se asignarán a los usuarios a través de capas. Las políticas de superior tienen prioridad que las inferiores.
68. La siguiente serie de temas le guía a través de las configuraciones de políticas utilizando la analogía de parar en tiendas especializadas para personalizar y afinar los motores de sus políticas.
69. Las políticas que se pueden aplicar se describen en los siguientes subapartados.

5.4.1 BYPASS

70. Tan importante como considerar lo que pasa por la plataforma de WPS es considerar lo que no debería pasar. Evitar que los destinos que no requieren seguridad pasen por los motores de políticas de WPS garantiza que los informes derivados de las transacciones de políticas no contengan información innecesaria. Además, esto mantiene que los motores de políticas estén funcionando de forma eficiente.
71. Considere los siguientes destinos típicos a evitar VPNs; sitios internos y direcciones IP (como intranets); sitios de confianza; o cualquier destino que sesgaría los informes de uso de la web. En ocasiones, puede añadir temporalmente una dirección IP o entrada de dominio a la lista de bypass mientras soluciona un problema de conexión.
72. Las mejores prácticas recomendadas por Symantec sobre estas políticas son:
    a) Cuando cree una entrada de desvío, facilite una descripción en los comentarios.
    b) Mantenga la lista lo más corta y manejable posible. Por ejemplo, cree objetos de lista que contengan todas las direcciones IP de prueba en lugar de crear entradas individuales.
    c) Programe y realice auditorías periódicas de las listas para asegurarse de que se satisfacen todas las necesidades de la empresa.
73. Para configurar esta política hay que realizar los siguientes pasos:
    a) Acceder a la consola de gestión de WPS.
    b) Seleccionar política de bypass y clicar añadir el tráfico que no se quiere investigar. Puede ser o IP/Subredes o dominios. Para este último ejemplo, se muestra como seria:

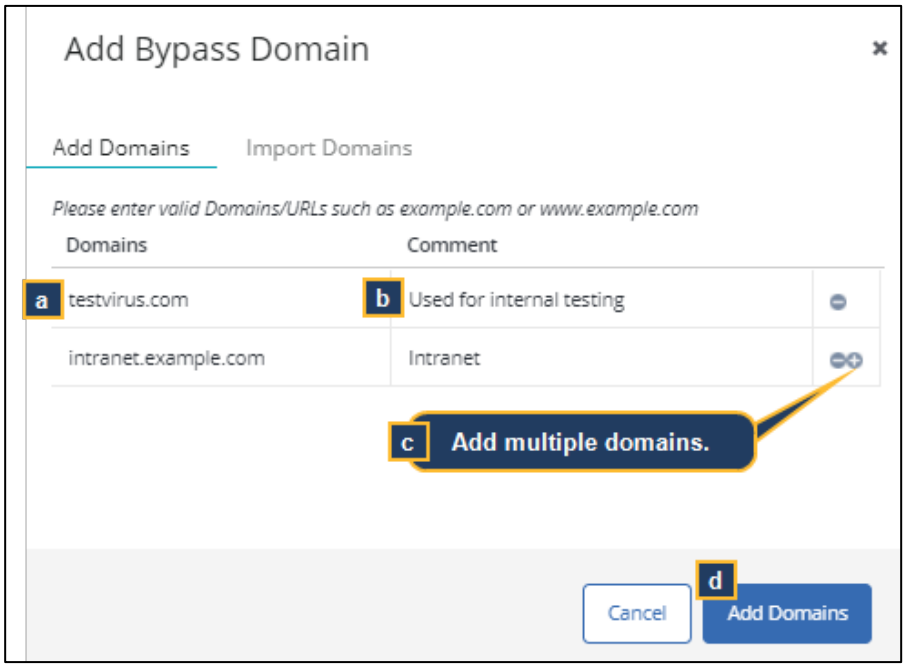

Ilustración 12. Dominio bypass

c) Hacer click en añadir dominio

d) Se abre un dialogo donde indicamos el o los dominios a descartar

e) Hacer click en Añadir.

f) Guarda la política

74. Para más información sobre cómo hacerlo con IPs/subredes, es de manera similar, pero clicando en añadir IPs/subredes:

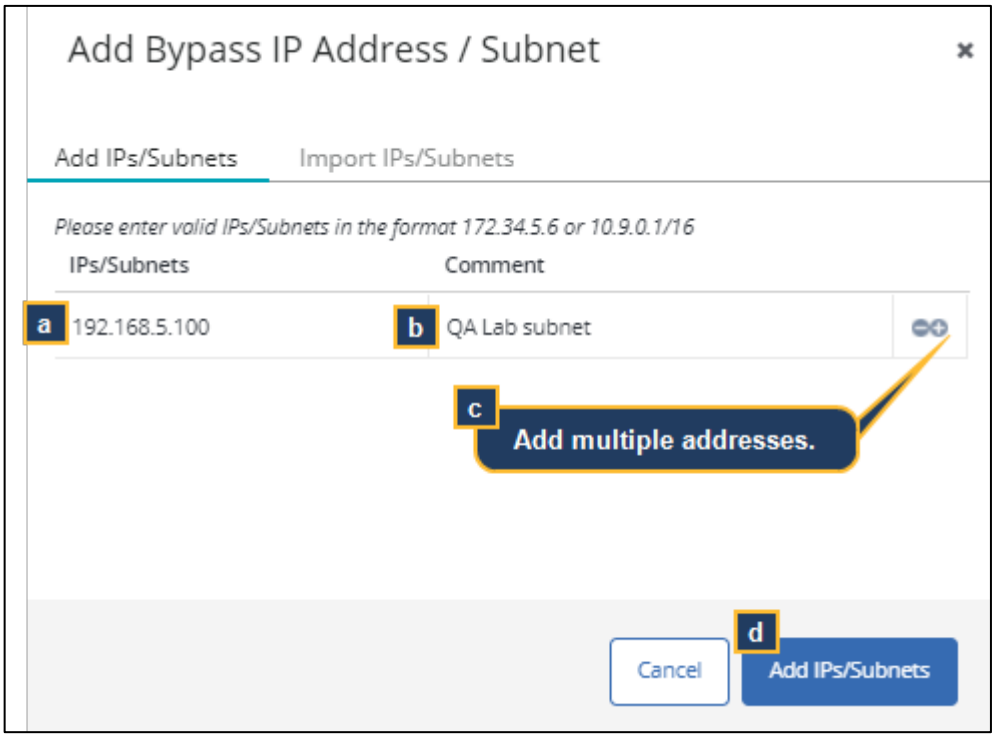

Ilustración 13. Bypass IPs / Subredes

75. Para más información sobre esta política puede acudir a las siguientes referencias:

    a) Política Bypass [REF5].

    b) Bypass Dominio [REF6].

    c) Bypass IP/Subredes [REF7].

5.4.2 TLS/SSL INTERCEPTION

76. Por defecto, la plataforma de WPS no intercepta el tráfico HTTPS entrante de las ubicaciones y aplicaciones web de destino. Con la configuración predeterminada, WPS aplica la política de filtrado de contenidos en la mayor medida posible. Sin embargo, Cloud SWG no puede aplicar políticas a operaciones que requieran una inspección más profunda, como controles de aplicaciones web o análisis de malware. La habilitación de la interceptación TLS/SSL permite el Servicio de Inteligencia de Amenazas (TIS). TIS realiza una inspección de nivel profundo en Cloud SWG para examinar el contenido en las conexiones HTTPS descifradas, y realiza comprobaciones de políticas.

77. El motor de políticas SSL proporciona la flexibilidad necesaria para realizar excepciones específicas al escaneado de nivel más profundo, lo que permite equilibrar la balanza de la privacidad y la seguridad. En la mayoría de las organizaciones, los sitios web financieros y sanitarios conocidos están exentos de la inspección SSL para proteger la privacidad de sus usuarios finales. Por defecto, Cloud SWG no intercepta lo siguiente:

    a) Tráfico HTTPS categorizado como Broker/trading, servicios financieros y salud, porque este contenido suele implicar información privada y sensible de cuentas personales.

b) Aplicaciones que aparecen en la lista SSL Bypass List o en la lista Mobile App Bypass porque se sabe que su tráfico se interrumpe debido a problemas de anclaje de certificados.

78. Además de las exenciones predeterminadas, su organización puede elegir o estar obligada a eximir otras categorías, grupos o incluso destinos web específicos de la interceptación SSL de la siguiente manera:

a) Acceda al portal de WPS

b) Seleccione la pestaña de politicas.

c) Abra la política de TLS/SSL Interception Policy

d) En la fila 3, hacer click en el lápiz como muestra la imagen:

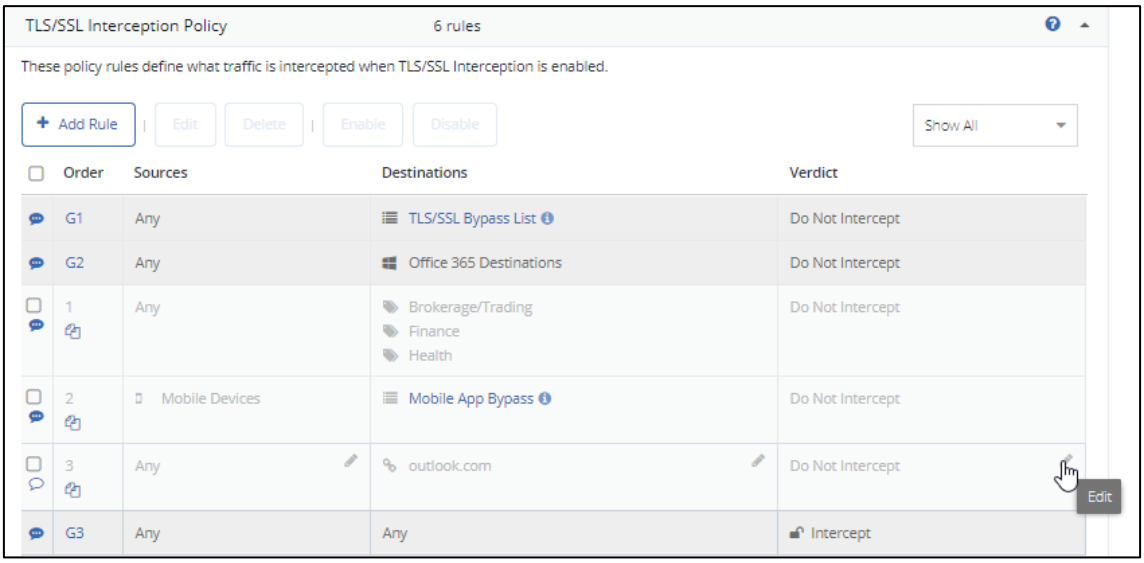

Ilustración 14. Polítitica de intercepción TLS

e) Añada el servicio en la columna “Destinations”. Existen varias formas de añadirla. En la siguiente imagen se muestra añadiendo como dominio.

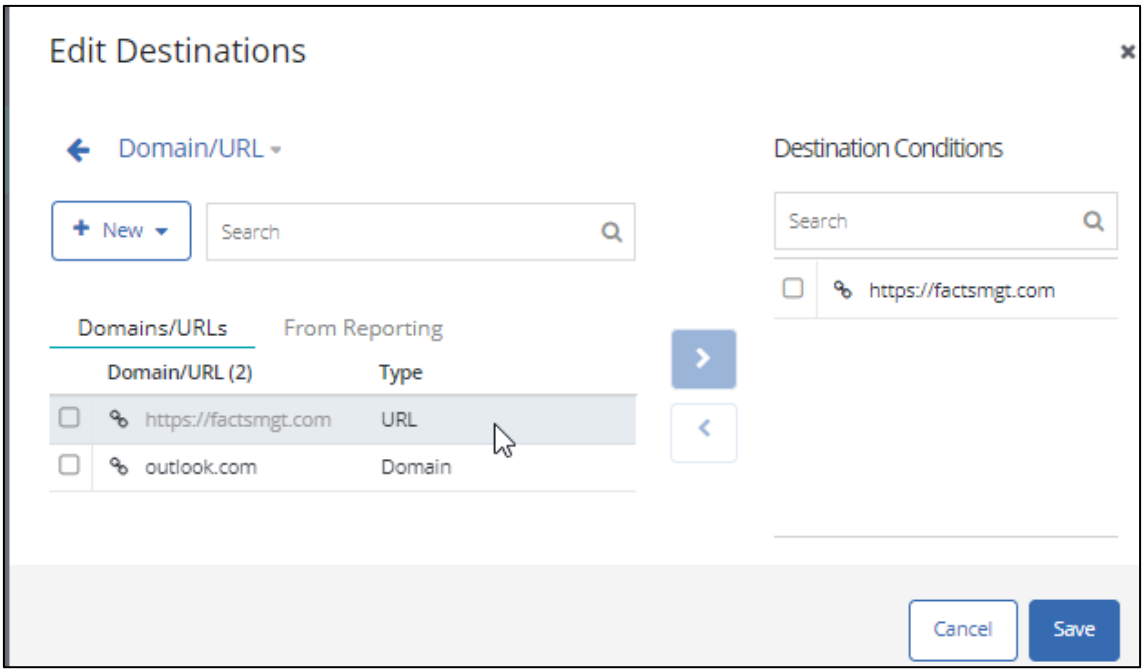

Ilustración 15. Añadiendo servicio como dominio

79. Guarda y aplica la política. En el caso que la política de TLS/SSL no esté operativa, tendrá que activarla.

80. Para más información sobre esta política, puede acudir a [REF8].

5.4.3 AUTHENTICATION EXEMPTIONS

81. Algunos problemas de red o decisiones empresariales pueden requerir que determinadas fuentes estén exentas de autorización a alguno o determinados destinos. Los métodos de autenticación de portal cautivo o SAML, que son métodos basados en la redirección, muestran una ventana independiente para que los usuarios introduzcan sus credenciales para continuar. Algunos problemas de red pueden impedir que los sistemas cliente muestren estas ventanas, como, por ejemplo:

    a) Problemas relacionados con CORS.

    b) Autenticación en bucle con servidores IdP basados en la nube.

    c) El dispositivo de origen (por ejemplo, un servidor heredado) no es compatible con la autenticación basada en redireccionamiento.

    d) La llamada a la API de una aplicación web no es compatible con la autenticación basada en redireccionamiento.

82. Para mitigar esto, añada destinos y orígenes que desee que estén exentos de los desafíos de autorización. Para añadir este servicio solo hay que seguir los siguientes pasos:

    a) Acceda a la consola de gestión de WPS.

    b) Seleccione la pestaña de políticas.

    c) Abra la política de Authetication Examption.

d) Hacer click en “Add Auth Exemption” y añade la información sobre el servicio a excepcionar.

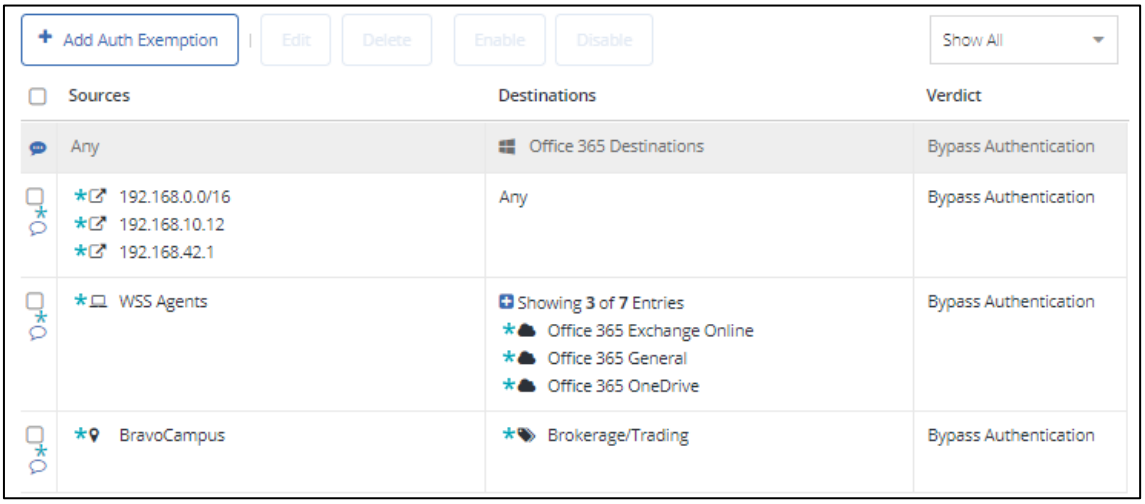

Ilustración 16. Añadiendo excepciones de autenticación

5.4.4 LOCATION

83. La Política de autenticación de SWG de Nube le permite definir el método de autenticación empleado en función de la ubicación fija del Firewall/VPN (IPsec) o del Proxy explícito. Esto es útil cuando se tiene una mezcla de métodos de autenticación.
84. Para acceder a esta política, hay que seguir los siguientes pasos:
    a) Primero, acceder a la consola de gestión de WPS
    b) Hacer click en la sección de políticas y selecciona la política de Location.
    c) Consta de tres campos a rellenar.
        - Método de acceso, que indica la forma de acceder
        - Fuente, a quien aplica este método
        - Autenticación. Tipo de identificación necesaria para acceder
85. Para que quede más claro, un ejemplo. Una empresa quiere que el Auth Connector proporciona autorización y autenticación para todas las conexiones a través de dispositivos de cortafuegos locales, pero emplea un IdP SAML para ubicaciones remotas que se conectan a través de Proxy explícito. O bien, si una ubicación no tiene acceso a un conector de autenticación o a un IdP SAML, active el portal cautivo.
86. Para este caso ejemplo, la política de “Location” debería de ser:

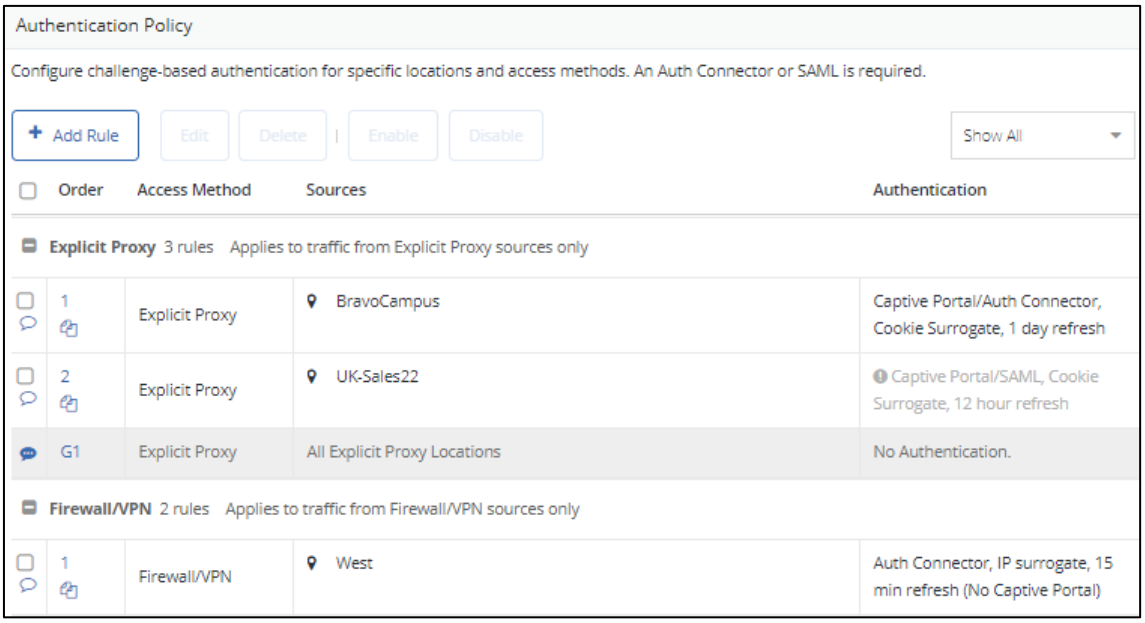

Ilustración 17. Política de autenticación

87. Para más información sobre esta política, puede acudir a [REF9].

5.4.5 CONTENT FILTERING

88. El Editor de Políticas de Filtrado de Contenidos es donde usted da forma a sus políticas de uso aceptable de la Web. Para garantizar el cumplimiento y la seguridad, defina políticas que restrinjan o permitan elementos de red y web como direcciones IP, categorías de filtrado de contenidos, aplicaciones web y las acciones a tomar cuando un usuario acceda a dicho contenido.

89. Para configurar la política de Content Filtering, hay que seguir los siguientes pasos:

    a) Acceder a la consola de gestión de WPS

    b) Hacer click en la pestaña de política de Content filtering.

    c) En este punto existen varios campos a rellenar dependiendo de la política a crear. Estos campos son los siguientes:

        - Sources. Quien solicita el contenido. Por defecto es “any”
            - Usuarios, Usuarios no autenticados, Grupos, Direcciones IP/Subredes, Ubicaciones fijas, Agentes y Usuarios móviles.
            - Geolocalizaciones
        - Destino
            - Contenido y límites. La condición se aplica a los parámetros del contenido. Por ejemplo, configure la política para que sólo se aplique a determinados tipos de archivos, navegadores o acciones dentro de aplicaciones web.
            - Acciones, como cargar y descargar archivos multimedia, participar en reuniones y juegos.
            - Tipo de fichero

- Horario, o cuándo se aplican las normas de la política, como el horario de oficina

- Veredicto. Es la acción a tomar respecto al contenido
  - Permitir o bloquear la solicitud o el contenido si se produce alguna coincidencia de políticas en la regla
  - Advertir (entrenar) a los empleados de que su actividad en Internet queda registrada
  - Redirigir al usuario a otra ubicación web (como un sitio de intranet que enumere las directrices de uso adecuado de la web)
  - Exigir una contraseña para acceder al contenido.

90. Un caso de uso para explicar mejor el generador de políticas de filtrado de contenido sería el siguiente:

91. Tras revisar los informes, una empresa ha descubierto que demasiados empleados consumen horas de trabajo jugando a juegos online y el departamento de seguridad informática añade una regla para bloquear la categoría Juegos. Sin embargo, discusiones posteriores revelaron que una simple regla de bloqueo global no sería suficiente. Ciertos trabajadores necesitan acceder a sitios de juegos. Además, el grupo de Marketing suele organizar reuniones sociales con los clientes al término de los seminarios de formación. Esto incluye competiciones de juegos para ganar premios.

92. La siguiente imagen muestra como habría que configurar las políticas en el editor de reglas:

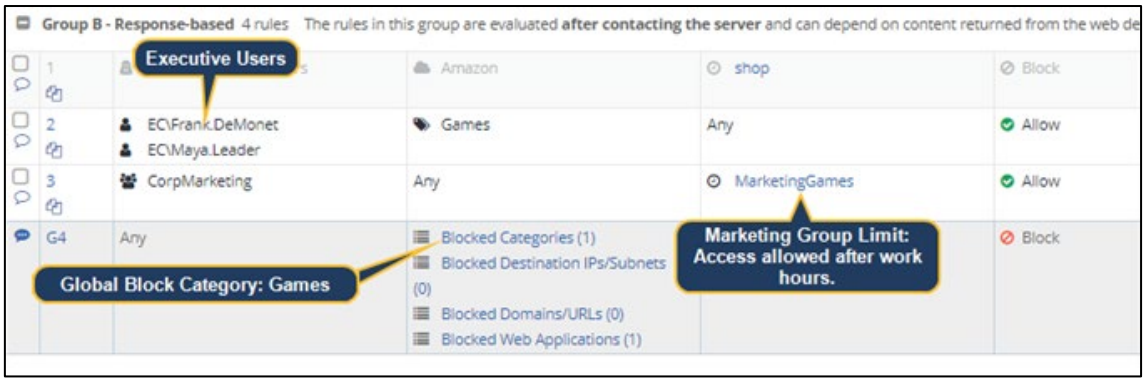

Ilustración 18. Políticas de filtrado de contenido

93. Dentro de esta política, existen una gran cantidad de elementos a tener en cuenta como aplicaciones cloud, categorías, tipo de usuarios etc. Por ello, para cualquier duda a la hora de la creación de esta política recomendamos acudir a la guía de administración del producto. En concreto a la parte de Content Filtering [REF10].

5.4.6 THREAT PROTECTION

94. Cuando se produce una transacción web, la solicitud ha llegado a la solución WPS (si no se encuentra en la lista Bypass) y ha continuado a través de las políticas de filtrado de

contenido y categorías. A continuación, la política Cloud SWG realiza comprobaciones en el Servicio de Inteligencia sobre Amenazas (TIS). Si la solicitud incluye un objeto como un archivo, un fichero CCS o JavaScript, el TIS busca el hash generado a partir del objeto y lo analiza.

95. Sin ninguna configuración adicional, el SWG en la nube ofrece protección contra programas maliciosos y contenidos web malintencionados diseñados para dañar las redes u obtener información privada de los usuarios. El servicio utiliza la Red Global de Inteligencia (GIN), impulsada por una comunidad de usuarios que se cuenta por decenas de millones. A medida que estos usuarios navegan por los contenidos web, los contenidos escaneados reciben una clasificación por categorías. La base de datos se actualiza en tiempo real. La política de SWG en la nube consulta esta base de datos.

96. La política de filtrado de contenidos predeterminada e inalterable impide el acceso a sitios web de contenido malicioso. Estas categorías bloqueadas se encuentran en estos subgrupos:

    a) Problemas de seguridad: como, por ejemplo, spam

    b) Amenazas a la seguridad: entre los que destaca datos salientes, maliciosos/botnets, phishing, evasión de proxy.

    c) Cuestiones de responsabilidad: como pornografía infantil entre otros.

97. Malware Analysis funciona con su política de filtrado de contenidos. Por ejemplo, la política de filtrado de contenidos permite una solicitud a la categoría de medios sociales, pero Malware Analysis detecta entonces que el archivo solicitado contiene un virus, se deniega la descarga y el cliente recibe una página de excepción en la que se explica la denegación.

98. Las licencias adicionales proporcionan sandboxing en tiempo real, capacidades de detonación posteriores a la entrega y notificaciones al administrador.

99. Dentro de esta política, existe el Editor de políticas de protección frente a amenazas para personalizar aún más su estrategia de protección. Puede crear diferentes tipos como, por ejemplo:

    a) Elegir una estrategia de protección de tipo de archivo más fuerte para los usuarios móviles.

    b) Permitir a usuarios o grupos específicos el acceso a categorías bloqueadas permanentemente.

    c) Permitir el acceso a contenido no categorizado.

    d) Definir políticas que dependan de múltiples condiciones. Por ejemplo, las reglas se activan si un grupo específico que accede desde una ubicación específica (construcción AND). También puede crear construcciones OR.

100. Para llegar a este editor de políticas, hay que seguir los siguientes pasos:

    a) Acceder a la consola de gestión de WPS

    b) Hacer click en la pestaña de Políticas

    c) Seleccione la política de Threat Protection

    d) Añade una regla

e) A la hora de crear la política, como ocurre en otras políticas, existen campos a rellenar:

- Sources. Quien solicita el contenido. Por defecto es “any”
  - Usuarios, Usuarios no autenticados, Grupos, Direcciones IP/Subredes, Ubicaciones fijas, Agentes y Usuarios móviles.
  - Geolocalizaciones
- Destino
  - Contenido y límites. La condición se aplica a los parámetros del contenido. Por ejemplo, configure la política para que sólo se aplique a determinados tipos de archivos, navegadores o acciones dentro de aplicaciones web.
  - Acciones, como cargar y descargar archivos multimedia, participar en reuniones y juegos.
  - Tipo de fichero
  - Horario, o cuándo se aplican las normas de la política, como el horario de oficina
- Veredicto. Es la acción a tomar respecto al contenido
  - Permitir o bloquear la solicitud o el contenido si se produce alguna coincidencia de políticas en la regla
  - Advertir (entrenar) a los empleados de que su actividad en Internet queda registrada
  - Redirigir al usuario a otra ubicación web (como un sitio de intranet que enumere las directrices de uso adecuado de la web)

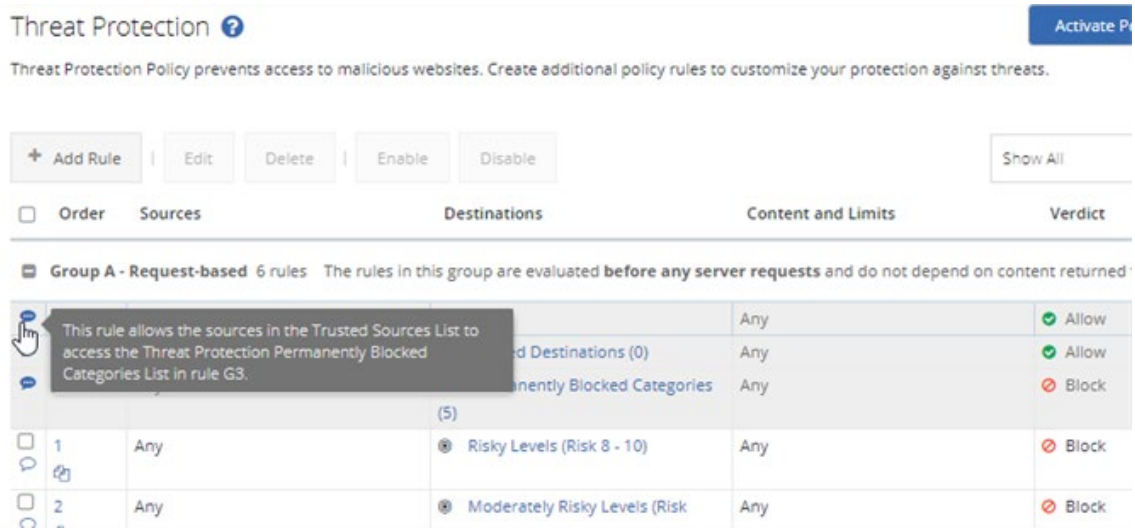

Ilustración 19. Politica Threat Protection

101. Al igual que ocurre con la política anterior, esta configuracion es bastante flexible y existen un gran número de parámetros que se puedes configurar. Para ello, se recomienda acudir a la documentación del producto, en especial a la política de Threat Policy [REF11].

5.4.7 RISK SCORE

102. La política por puntuación de riesgo es una extensión de la política de protección frente a amenazas. La red de Global Intelligence Network, que rellena las bases de datos de categorías de contenido de WPS, también proporciona puntuaciones de riesgo asignadas a todos los sitios web. Las puntuaciones van de 1 a 10. Un sitio con una puntuación de 1 se considera muy probablemente seguro, mientras que una puntuación de 10 es maliciosa. Esto le permite definir políticas de amenazas aún más granulares.

103. Esta política se configura de la misma forma que la política de Threat Protection.

    a) Acceda a la consola de gestión de WPS

    b) Entre en la pestaña de políticas y seleccione la política de Threat Protection

    c) Cuando cree una regla, podrá seleccionar en el campo de destino, la puntuación.

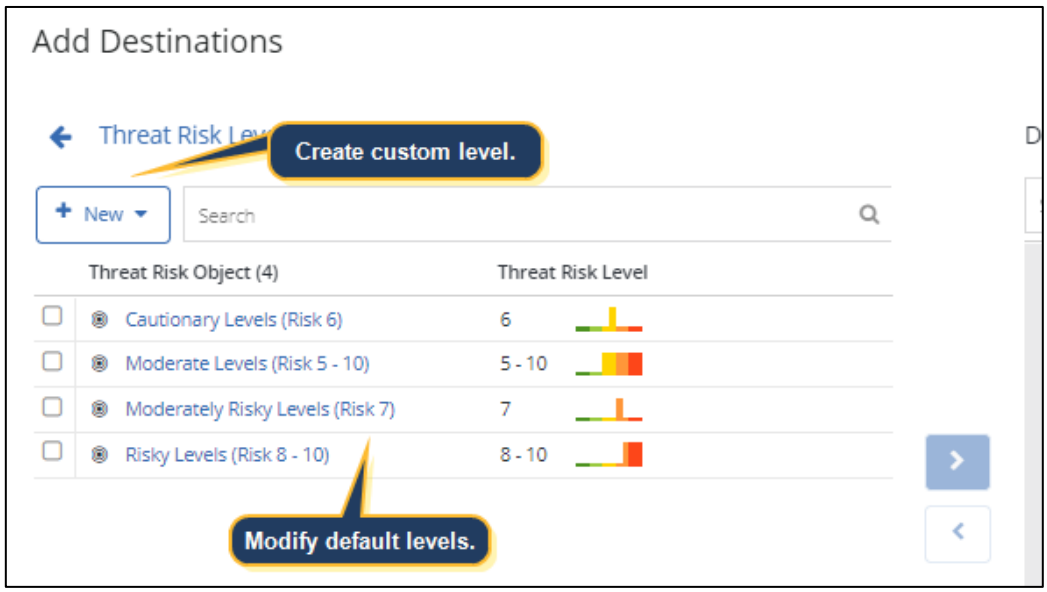

Ilustración 20. Risk score

104. Dependiendo de esta categorización, podrá decidir qué acción tomar cuando un usuario acceda a una web. El ejemplo de la política se muestra en la siguiente imagen, a partir de la regla G3:

Ilustración 21. Política por puntuación de riesgo

105. Para mas informacion sobre esta política, acuda a la documentación publicada, en concreto a la política de Risk Score [REF12].

5.4.8 GEOLOCALIZACION

106. Le permite crear políticas basadas en: desde qué país o hacia qué país se produce una solicitud de contenido. Bloquee sitios potencialmente no deseados si la política corporativa no permite transacciones comerciales con determinados estados nación. Esto también es valioso a efectos de elaboración de informes e investigación si se detecta tráfico inusual con destino a un estado nación específico. Cree un subconjunto granular de reglas que permitan o bloqueen en función de la política corporativa requerida.

107. Dentro de la política de filtrado de contenido y control de amenazas, existe la posible de añadir la localización de la fuente o el destino web. En la imagen se muestra:

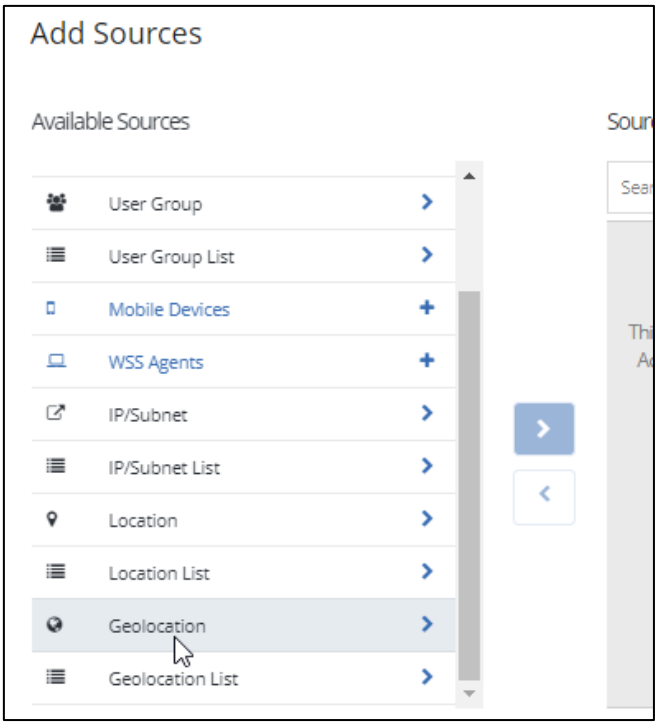

Ilustración 22. Añadiendo localización

108. Para más información sobre esta política, acuda a la documentación publicada, en concreto a la política de geolocalización [REF13].

5.4.9 WEB ISOLATION

109. Web Isolation es una solución sin que no necesita agente instalado que permite a los empleados navegar por Internet de forma segura en cualquier dispositivo y con cualquier navegador. Se permiten todas las solicitudes, pero Web Isolation ejecuta las sesiones web lejos de los dispositivos de los usuarios. Las páginas web se renderizan y aíslan como gráficos para su visualización en el navegador del usuario final. Aislar el contenido impide que el malware llegue a la red y a los dispositivos. Un caso de uso común es proteger a los empleados que navegan por sitios no categorizados y potencialmente maliciosos.

110. La política de Web Isolation es similar a las otras políticas. Dependiendo de donde se navegue, el veredicto será permitir o no permitir el Web Isolation:

    a) Permitir: WPS ejecuta la solicitud web en un entorno seguro y aislado y realiza el análisis de malware de Web Isolation.

    b) No permitir: WPS omite Web Isolation y sirve la respuesta como contenido web completo.

111. Para configurar esta politica, hay que seguir los siguientes pasos.

    a) Acceda a la consola de gestión de WPS.

    b) Hacer click en la política de Web Isolation

    c) Añade una regla. En esta regla hay que añadir dos elementos, condición y veredicto.

    d) Dentro de la condición, se puede elegir parámetros como :

- Fuente. Quien hace la petición de tráfico. Existe una gran colección de parámetros a elegir, entre los que están usuarios, grupo, tipo de dispositivos etc.

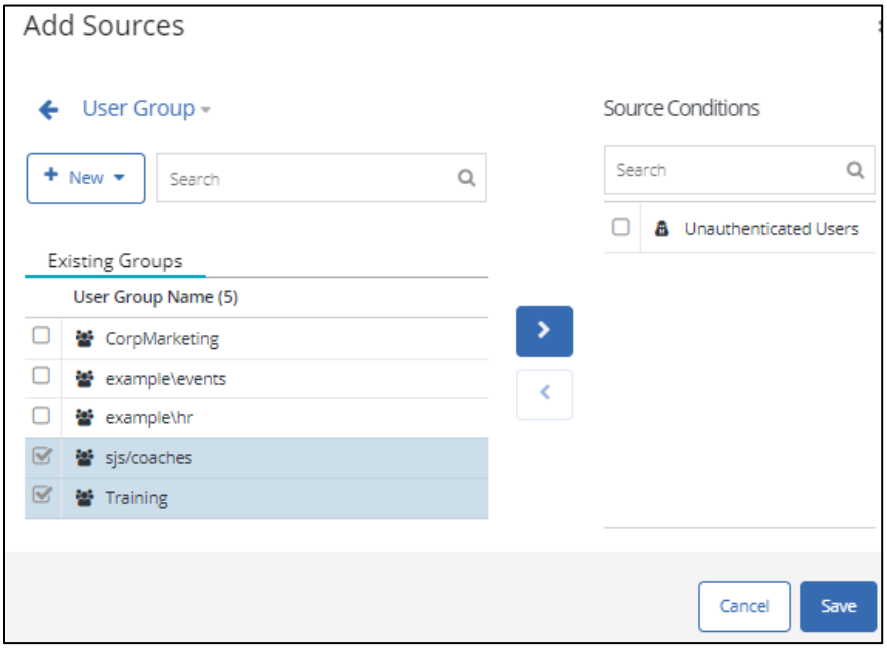

Ilustración 23. Añadir source en Web Isolation

- Contenido. Tipo de tráfico a monitorizar.
- Destino. Información de donde se encuentra el tráfico requerido.

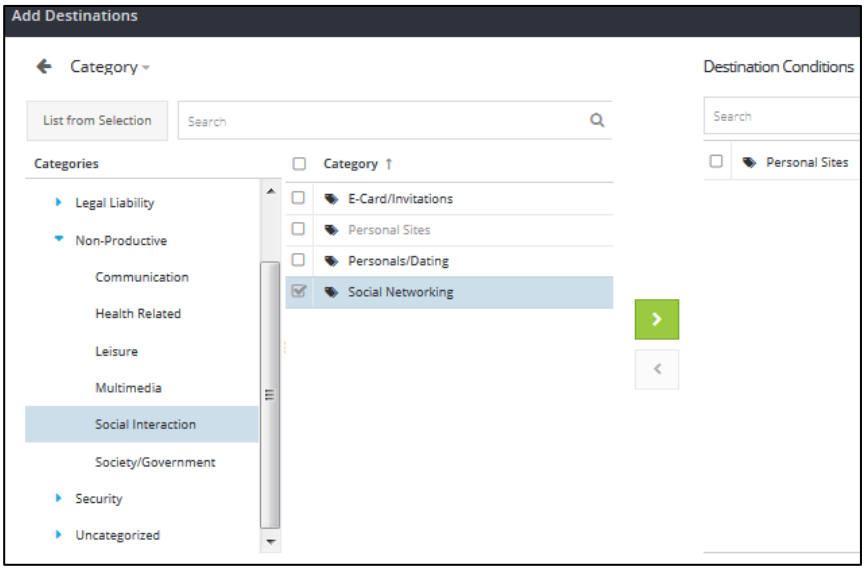

Ilustración 24. Añadiendo destino en Web Isolation

e) Una vez se ha configurado la condición, se aplica el veredicto, que puede ser si se realiza la opción de aislar o no.

112. Una opción que se recomienda es usar el modelo de risk score junto a web isolation. Para ello, se recomienda hacer isolation en el nivel 7. Para configurar esta opción:

a) Hay que marcar en la pestaña destino, risk score igual a 7.

b) Marcar como veredicto Isolation.

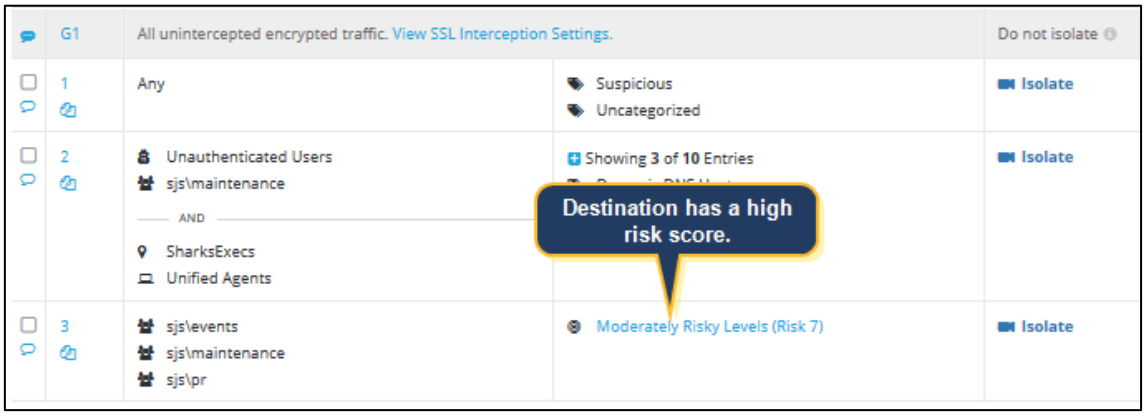

Ilustración 25. Isolation y Risk Score

5.4.10 HEADER MODIFICATION

113. Las políticas de Header Modification modifican las peticiones ascendentes, permitiéndole mantener conexiones de cliente que se adapten a los requisitos de su red. Se pueden añadir, borrar o editar una cabecera.

114. Los pasos a seguir para la configuración de esta política son los siguientes:

a) Navegue a la política de Header Modification.

b) Añada regla en el apartador de Specific Header Rules.

c) Defina la regla de condición.

d) En la sección de veredicto, indique que quiere hacer, borrar, añadir o modificar:

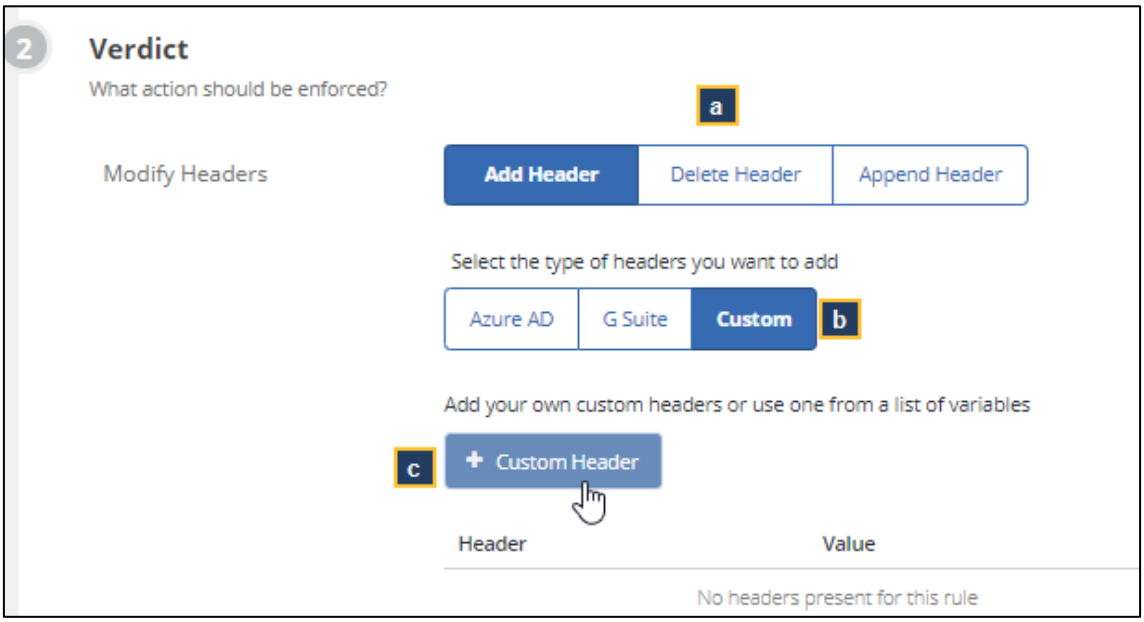

Ilustración 26. Estableciendo modificadores de cabeceras.

e) Hay de tres tipos, de Azure AD, GSuite o custom, que te permite crear la cabeza que quieras. Si seleccionamos custom, aparecerá el siguiente dialogo:

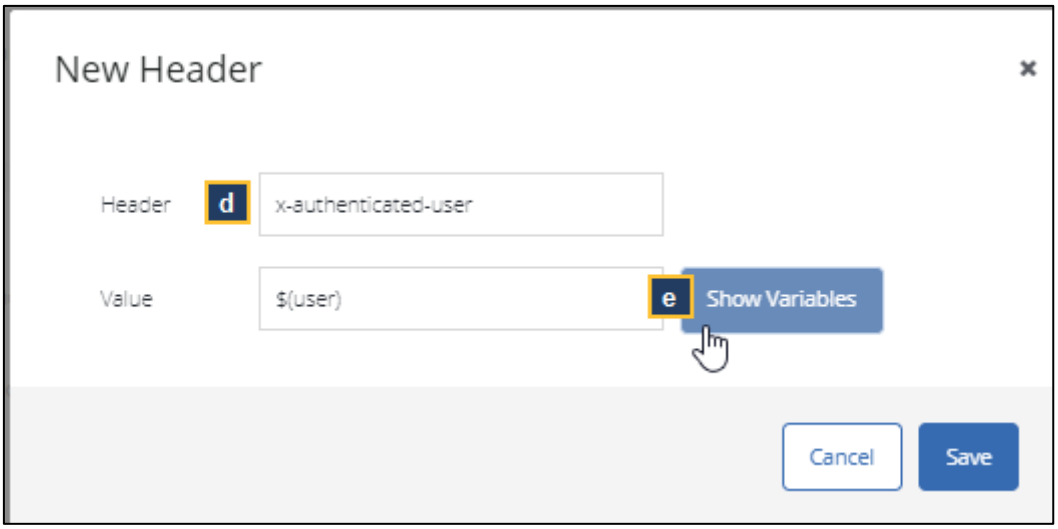

Ilustración 27. Creando una cabezera personalizada

f) Una vez este creado el veredicto, hacer click en Save.

5.5 ACTUALIZACIONES

115. Al tratarse de una solución en la nube, la gestión de actualización de la consola es automática. Cada cierto intervalo, normalmente una vez al mes, se realiza una actualización de la consola de gestión.

116. Toda la información relacionada con la actualización de consola se puede consultar en el siguiente enlace. Además, en el portal de soporte, se puede configurar para recibir alertas de cuando hay planeado hacer la actualización y que nuevas funcionalidades se han añadido.

117. De no tener configurado esta opción, al hacer login por primera vez tras una actualización, le aparecerá un dialogo donde indica la nueva versión y le indica que nuevas funcionalidades hay añadidas, además de donde poder consultar dicha información.

5.6 BACKUP

118. Al igual que el apartado anterior, al tratarse de un servicio en la nube, el cliente no tiene que preocuparse por realizar el backup de la solución. Automáticamente se realizarán tareas de mantenimiento para tener esta funcionalidad activa.

5.7 AUDITORÍA

5.7.1 REGISTRO DE EVENTOS

119. A medida que se produce el tráfico de Internet, Cloud SWG registra cada transacción en los registros de acceso, que se almacenan en los centros de datos de Symantec. WPS toma los datos de varios campos relevantes de los registros de acceso para generar informes.

120. Los campos dentro de los registros de eventos son los siguientes:

Extended Log Format	Description
application-name	Alias selected from the application name (x-bluecoat-application-name).
c-ip	Client IP address.
c-ip-subnet	Subnet of the client IP (c-ip).
c-ip-version	IP version of the client address (IPv4 or IPv6).
cs(referer)	Content of request header referer.
cs(user-agent)	Content of request header User-Agent
cs(x-requested-with)	Content of request header X-Requested-With.
cs-auth-group	A single group to which an authenticated user belongs. If a user belongs to multiple groups, this field is empty and cd-auth-groups is populated instead.
cs-auth-groups	List of groups that an authenticated user belongs to. Only groups that are referenced by policy are included.
cs-bytes	Number of HTTP/1.1 bytes sent from the client to the appliance.
cs-categories	All content categories of the request URL.
cs-host	Hostname from the client request URL. If URL rewrite policies are used, the value of this field is derived from the log URL.
cs-icap-error-details	REQMOD ICAP error details.
cs-icap-service	REQMOD ICAP service or service group name.
cs-icap-status	ICAP REQMOD status.
cs-method	Request method.
cs-threat-risk	Threat risk level of the request URL.
cs-uri-extension	Document extension from the original requested URL.
cs-uri-path	Path from the log URL, not including the query.
cs-uri-port	Port from the log URL.
cs-uri-query	Query from the log URL.
cs-uri-scheme	Scheme from the log URL.
cs-user-domain	Domain name from cs-userdn.
cs-userdn	Full username of a client authenticated to the proxy (fully distinguished).
cs-version	Protocol and version from the client request, such as “HTTP/1.1".
cs(X-Forwarded-For)	Content of request header X-Forwarded-For.
date	GMT date in YYYY-MM-DD format.
isolation-url	The Web Isolation service URL.
ma-detonated	Indicates whether the content was sent to Malware Analysis for detonation. Possible values are 0 or 1.

Extended Log Format	Description
page-views	Indicates whether the URL was typed manually by a user in the browser. Possible values are 0 or 1.
r-ip	IP address from the outbound server URL.
r-ip-version	IP version of the outbound server address (IPv4 or IPv6).
r-supplier-country	Reports the country of the IP address to which Cloud SWG connected. The country of the first IP address returned from a DNS resolution of the server URL host. For example, if the transaction was denied based on an earlier condition such as URL category, the field indicates the country that the service tried to connect to first.
risk-groups	Threat Risk Level group that is based on the request URL categories (cs-categories).
rs(content-type)	Content of request header content-Type.
rs-icap-error-details	ICAP RESPMOD error details.
rs-icap-service	RESPMOD ICAP service or service group name; available when the response is served from cache.
rs-icap-status	ICAP RESPMOD status.
rs-version	Protocol and version of the response from an upstream host to the proxy, such as “HTTP/1.1".
s-action	The action the appliance took to process the request. Possible values include: ALLOWED, DENIED, FAILED, SERVER_ERROR, ISOLATION_CS (A request from the browser was sent to the Web Isolation service.), ISOLATION_INITIATED (The session was isolated due to an Isolate verdict in policy.), ISOLATED_DOCUMENT (The document was isolated due to a Document Isolate verdict in policy).
s-ip	IP address of the appliance on which the client established its connection.
s-source-ip	Source IP used by the proxy.
s-supplier-country	The geolocation (country) associated with the IP address of the connection, which is identified by s-supplier-ip. This location is only set if a connection is made, or if an exception does not occur.
s-supplier-failures	A list of entries where the IP address resolved but did not result in a successful connection. Each entry comprises the IP address, country, and whether the connection was denied or timed out. This field is designed for use with Symantec Reporter
s-supplier-ip	IP address used to contact the upstream host. This address is only set if a connection is made, or if an exception does not occur.

Extended Log Format	Description
sc-bytes	Number of HTTP/1.1 bytes sent from the appliance to the client.
sc-filter-result	Content filtering result, such as DENIED, PROXIED or OBSERVED
sc-status	Protocol status code from the appliance to the client.
search-terms	Text entered in the browser search engine, based on cs-host and cd-uri-query
time	GMT time in HH:MM:SS format.
time-taken	Time taken (in milliseconds) to process the request. The time is measured from the first byte of client request data that is received by the proxy, to the last byte sent by the proxy to the client. The time includes delays by ICAP, and so on.
verdict	Policy verdict of block or allow, based on sc-status and x-exception-id.
x-bluecoat-access-type	Method used to access the cloud service.
x-bluecoat-appliance-name	Configured name of the appliance.
x-bluecoat-application-name	Reports the application name.
x-bluecoat-application-operation	Reports the operation of an application.
x-bluecoat-location-id	ID of the cloud service customer site.
x-bluecoat-location-name	Cloud service location name of the edge SWG appliance
x-bluecoat-reference-id	Reference ID specified in the referece_id (Rule_ID) action in a policy rule.
x-bluecoat-request-tenant-id	Tenant ID for the request.
x-bluecoat-placeholder	A placeholder represented by a dash (-)
x-bluecoat-transaction-uuid	Globally unique per-request identifier generated by the appliance. Default exception pages include the transaction ID. You can look for the ID in the access log to learn more about the transaction.
x-client-agent-sw	Client agent software.
x-client-agent-type	Agent type of the authenticated client.
x-client-device-id	A unique identifier for the client device.
x-client-device-name	The name of the device.
x-client-device-type	Device type.
x-client-os	Client operating system.

Extended Log Format	Description
x-cloud-rs	Summary of RS server processing in the form (<rs-ratings>:<rating-source>:<rating-label>)
x-client-security-posture-details	Information that is related to how secure the client environment is per the compliance policy.
x-client-security-posture-risk-score	The risk score that indicates the security posture of the client.
s-computername	Configured name of the proxy
x-cs(referer)-uri-categories	All content categories that are associated with the referer header URL
x-cs-certificate-subject	Subject of the certificate presented by the client.
x-cs-client-ip-country	The country associated with the client IP address.
x-cs-connection-negotiated-cipher	OpenSSL cipher suite negotiated for the client connection.
x-cs-connection-negotiated-cipher-size	Cipher size of the OpenSSL cipher suite negotiated for the client connection.
x-cs-connection-negotiated-ssl-version	Version of the SSL protocol negotiated for the client connection.
x-cs-ocsp-error	An error was observed during the OCSP check for a client certificate.
x-cs-public-ip	Client public IP address.
x-data-leak-detected	Whether a data leak has occurred, according to the ICAP response.
x-dns-cs-address	The address that is queried in a reverse DNS lookup.
x-dns-cs-category	The category associated with the hostname that was sent to the DNS server.
x-dns-cs-dns	The hostname that is queried in a forward DNS lookup.
x-dns-cs-opcode	The DNS OPCODE used in the DNS query.
x-dns-cs-qclass	The DNS QCLASS used in the DNS query.
x-dns-cs-qtype	The DNS QTYPE used in the DNS query.
x-dns-cs-threat-risk-level	The Threat Risk Level of the hostname that was sent to the DNS server.
x-dns-cs-transport	The transport protocol used by the client connection in a DNS query.
x-dns-lookup-time	Total time taken (in ms) to perform the client DNS lookup.
x-dns-rs-a-records	The DNS A RRs in the response from upstream.
x-dns-rs-cname-records	The DNS CNAME RRs in the response from upstream.
x-dns-rs-ptr-records	The DNS A RRs in the response from upstream.
x-dns-rs-rcode	The DNS RCODE in the response from upstream.

Extended Log Format	Description
x-exception-id	Identifier of the exception resolved (empty if the transaction has not been terminated).
x-http-connect-host	The host name in the original HTTP CONNECT request.
x-http-connect-port	The port in the original HTTP CONNECT request.
x-icap-reqmod-header(x-icap-metadata)	ICAP REQMOD header details.
x-icap-respmod-header(x-icap-metadata)	ICAP RESPMOD header details.
x-random-ipv6	Static IPv6 address per tenant per internal IP address per hour. The value changes every hour and is produced by X-Forwarded-For header anonymization.
x-request-origin	Specifies the origin of a request with one of the following values: client (The request did not originate from the Web Isolation service.) and isolation (the request originated from the Web Isolation service).
x-rs-certificate-hostname	Hostname from the server TLS/SSL certificate.
x-rs-certificate-hostname-categories	All content categories of the server TLS/SSL certificate hostname.
x-rs-certificate-hostname-category	Single content category that is associated with the server SSL certificate hostname.
x-rs-certificate-hostname-threat-risk	Threat risk level of the server TLS/SSL certificate hostname.
x-rs-certificate-observed-errors	Errors observed in the server certificate.
x-rs-certificate-validate-status	Result of validating the server TLS/SSL certificate.
x-rs-connection-negotiated-cipher	OpenSSL cipher suite negotiated for the server connection.
x-rs-connection-negotiated-cipher-size	Cipher size of the OpenSSL cipher suite negotiated for the server connection.
x-rs-connection-negotiated-cipher-strength	Strength of the OpenSSL cipher suite that is negotiated for the server connection.
x-rs-connection-negotiated-ssl-version	Version of the SSL protocol negotiated for the server connection.
x-rs-ocsp-error	Errors that occurred during the OCSP check of the server certificate

Extended Log Format	Description
x-sc-connection-issuer-keyring	Issuer for forged certificates.
x-sc-connection-issuer-keyring-alias	Key alias name in the HSM issuer for forged certificates.
x-sr-vpop-country	Country of the egress IP.
x-sr-vpop-country-code	Country code of the egress IP.
x-sr-vpop-ip	Public egress IP address.
x-symc-dei-app	Application name that is set in the Cloud SWG policy.
x-symc-dei-via	Identifier for the Dedicated IP NAT proxy as rewritten by policy from the X-SYMC-DEI-Via header
x-symc-file-reputation-score	File Reputation Score from Malware Analysis (MA). This field is applicable if Cloud SWG has a MA license; otherwise, the field is empty.
x-symc-upload-source	Specifies the origin of a logged event with one of the following values: Datapath(The log line is from a Cloud SWG proxy.) hosted (the log line is from an on-premises Edge SWG(ProxySG) appliance.
x-timestamp-unix	Number of seconds since UNIX time (Jan 1,1970, in local time).
x-virus-id	Identifier of a virus if one was detected.D191:D218D188:D218D209D190:D21D15:D218

Tabla 10. Campos de los registros de eventos

5.7.2 REGISTRO DE EVENTOS DE ADMINISTRADORES

121. WPS registra cada vez que un administrador o usuario de la consola de gestión inicia y cierra sesión o realiza una acción, como editar o enviar por correo electrónico un informe. Los usuarios con rol de administrador pueden revisar estas transacciones. En el portal de WPS, seleccione Account Configuration -> Account Auditing. La página Auditoría de la cuenta muestra las acciones de usuario realizadas en la cuenta.

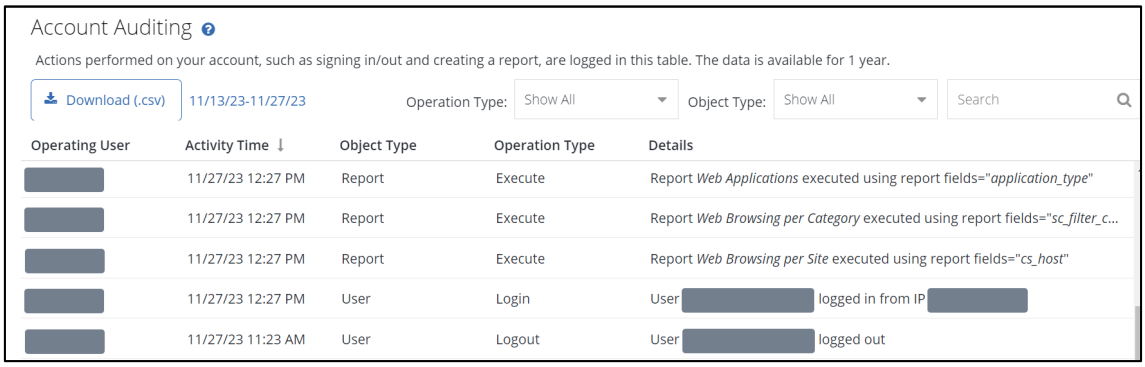

Ilustración 28. Auditoría de cuentas de usuarios

122. Puede realizar las siguientes tareas opcionales de.

    a) Filtra resultado por rango de fecha, tipo de operación o por objeto.

    b) Buscar por un elemento en concreto, como el nombre de un usuario o administrador.

    c) Descargar este registro de actividades en un fichero .csv.

5.7.3 ALMACENAMIENTO REMOTO

123. A medida que el WPS procesa las solicitudes y transacciones de tráfico web, almacena los registros de acceso por hora en el servicio. Este registro de eventos se guarda en las distintas localizaciones de nuestros data center. Este registro queda almacenado por un tiempo máximo de 100 días. A partir de llegar a este número, la solución empieza a borrar los eventos más antiguos.

124. Una opción que permite la solución de WPS es exportar los registros de eventos para que se guarden de manera local por parte del cliente. Existen diferentes formas de exportar estos datos.

5.7.3.1 EXPORTACION EN RAW

125. Cuando se descarga un registro de acceso desde el portal de WPS, el portal genera un archivo ZIP que contiene uno o varios archivos CSV o ELFF por hora (utilizando la marca de tiempo recibida) de datos. Cada nombre de archivo de registro tiene el siguiente formato:

    “logdownload-<tenant_id>yyyy-mm-ddTHH<unique_id>.<csv_or_elff>”

126. Para completar esta opción:

    a) En el portal de SWG en la nube, seleccione Account Configuration -> Log Export.

    b) Seleccione WPS como fuente de datos.

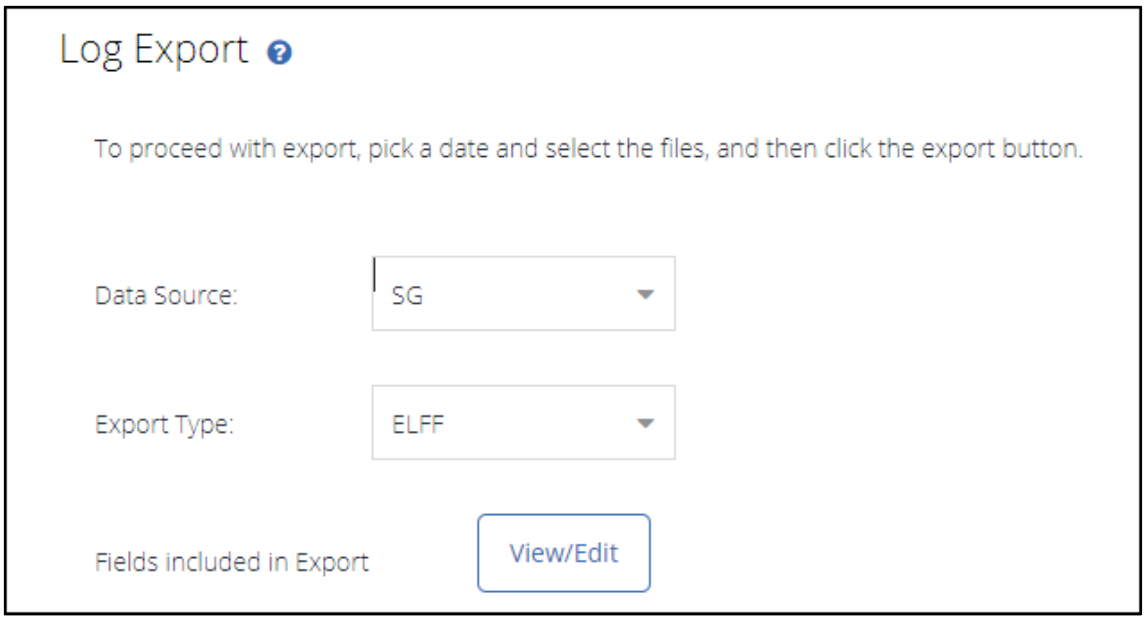

Ilustración 29. Exportación de registro de eventos

c) Especifique el formato de descarga que requiere su lector de registros externo. Opcionalmente, puede añadir o eliminar campos de registro de los archivos de registro de acceso descargados:

1. Seleccione el tipo, .CSV o ELFF
2. Hacer click en vista, para seleccionar el rango a exportar
3. Seleccione que campos a exportar
4. Guarda la configuración

d) En el área Available Files, utilice los filtros de fecha y hora para especificar el periodo de recogida de datos. El portal muestra los archivos correspondientes a la fecha y hora especificadas. La columna Tamaño muestra el tamaño de cada archivo.

e) Selecciona al menos uno para descargar y hacer click en Export.

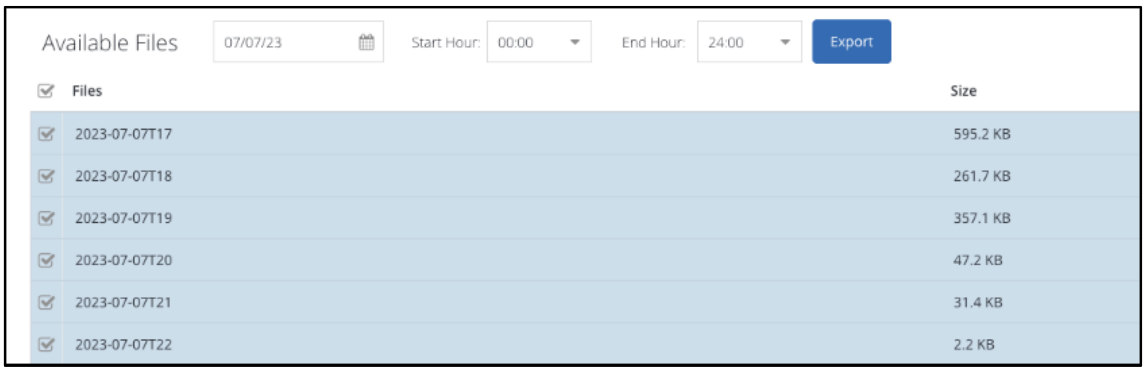

Ilustración 30. Selección de ficheros a exportar

5.7.3.2 NEAR REAL-TIME

127. La transmisión de eventos de SWG en la nube es la sucesora de la API Sync, que proporciona un servicio de transmisión de registros casi en tiempo real; sin embargo, la API requiere que proporcione scripts y programas cliente para comunicarse con la solución de WPS. La transmisión de eventos ofrece una escalabilidad mejorada, la posibilidad de utilizar salidas estándar y flexibles, y una mejor integración con las canalizaciones de datos modernas. Si actualmente utiliza la API de sincronización, considere la posibilidad de probar la función de transmisión por secuencias de eventos en el portal de SWG en la nube para disfrutar de una experiencia simplificada y flexible.

128. En el portal de WPS, configure canales para reenviar secuencias de eventos a un bucket de almacenamiento en la nube propiedad de la organización o para extraer eventos de un Kafka personalizado. Cada canal controla el formato, la entrega y otras propiedades de un flujo de eventos específico. Por ejemplo, cada canal especifica si los eventos están en formato ELFF (Extended Log File Format) o NDJSON (Newline Delimited JSON)

129. Puede configurar hasta 10 canales (incluidos canales habilitados y deshabilitados) para flujos de eventos. Como práctica recomendada, dedique cada canal a un propósito específico y añada campos que proporcionen datos para el contexto del canal. Una vez configurados los canales de eventos de WPS, puede utilizar un SIEM o enviar los datos a través de una canalización a su herramienta SOC para consumir los datos de eventos con fines de análisis forense, búsqueda de amenazas y cumplimiento de requisitos.

130. Para configurar un canal de eventos, realice los pasos siguientes:

a) En el portal de WPS, seleccione Account Configuration -> Event Streaming.

b) En el dialogo que aparece, seleccione Añadir.

c) Seleccione un canal de eventos para configurar. Existe diferentes configuraciones:

- AWS bucket
- Azure bucket
- GPC bucket
- Kafka.

6 REFERENCIAS

[REF1] Cloud Secure Web Gateway (Cloud SWG)
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help.html

[REF2] Guía de Seguridad de las TIC CCN-STIC 807, Criptología de empleo en el Esquema Nacional de Seguridad, Mayo 2022.

[REF3] Configure a password policy.
https://help.okta.com/en-us/content/topics/security/policies/configure-password-policies.htm

[REF4] Cloud SWG Connectivity
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/conn-matrix.html

[REF5] Configure Policy Bypasses
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/policy-matrix/wss-policy-route-bypass.html

[REF6] Prevent a Domain From Routing to Cloud SWG
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/content_filtering_sol/adm_bypassdomain_ta.html

[REF7] Prevent IP/Subnet From Routing to Cloud SWG
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/content_filtering_sol/adm_bypass_IPSubnet_ta.html

[REF8] TLS/SSL Interception in Cloud SWG
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/about_ssl_co.html

[REF9] Configure Authentication Policy
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/policy-matrix/wss-policy-route-auth.html

[REF10] Content Filtering Policy in Cloud SWG
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/content_filtering_sol.html

[REF11] Threat Protection
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/threat-protection.html

[REF12] Malware Policy Based on Risk Score
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/threat-protection/mw_riskpolicy.html

[REF13] Cloud SWG Geolocation Policies
https://techdocs.broadcom.com/us/en/symantec-security-software/web-and-network-security/cloud-swg/help/content_filtering_sol/about_geolocations.html

7 ABREVIATURAS

ADSI	Active Directory Service Interfaces
API	Application Programming Interface
AWS	Amazon Web Services
CMP	Cloud Management Portal
CORS	Cross-Origin Resource Sharing
CSV	Comma-Separated Values
CTC	Cloud Traffic Controller
DNS	Domain Name System
ELFF	Extended Log File Format
ENS	Esquema Nacional de Seguridad
GCP	Google Cloud Platform
GIN	Global Intelligence Network
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IdP	Identity Provider
IPsec	Internet Protocol Security
JSON	JavaScript Object Notation
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
MFA	Multi-Factor Authentication
NDJSON	Newline Delimited JSON
PAC	Proxy Auto-Config
RPC	Remote Procedure Call
SAML	Security Assertion Markup Language
SIEM	Security Information and Event Management
SMB	Server Message Block
SOC	Security Operations Center
SSL	Secure Sockets Layer
SWG	Secure Web Gateway
TCP	Transmission Control Protocol

TIS	Threat Intelligence Service
TLS	Transport Layer Security
UDP	User Datagram Protocol
WPS	Web Protection Suite
WSS	Web Security Service

PUBLICACIONES DE DEFENSA

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