paloalto TECHDOCS

Administración de Advanced URL Filtering

docs.paloaltonetworks.com

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- For the most recent version of this guide or for access to related documentation, visit the Technical Documentation portal docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

April 21, 2023

Table of Contents

Fundamentos de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

La tecnología de filtrado de URL protege a los usuarios de las amenazas basadas en la web al proporcionar un control granular sobre el acceso de los usuarios y la interacción con el contenido en Internet. Puede desarrollar una política de filtrado de URL que limite el acceso a los sitios en función de Categorías de URL, usuarios y grupos. Por ejemplo, puede bloquear el acceso a sitios que se sabe que alojan malware y evitar que los usuarios finales introduzcan credenciales corporativas en sitios de determinadas categorías.

Para obtener un control granular sobre el acceso de los usuarios a las categorías, puede crear un perfil de URL Filtering y definir el acceso al sitio para categorías de URL predefinidas y personalizadas; a continuación, aplique el perfil a las reglas de la política de seguridad. También puede usar categorías de URL como criterios de coincidencia en las reglas de la política de seguridad. Para obtener una lista de las formas en que una suscripción de Advanced URL Filtering puede satisfacer las necesidades de seguridad web de su organización, consulte Casos de uso de URL Filtering.

- Solución de filtrado de URL de Palo Alto Networks
- Compatibilidad con el filtrado de URL
- Categorización local en línea
- Cómo funciona Advanced URL Filtering
- Perfiles de URL Filtering
- Categorías de URL
- Casos de uso de URL Filtering

Solución de filtrado de URL de Palo Alto Networks

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Advanced URL Filtering (anteriormente URL Filtering) es un servicio de suscripción que protege su red y a sus usuarios frente a amenazas maliciosas y evasivas basadas en la web, conocidas y desconocidas. La suscripción proporciona la misma funcionalidad que el filtrado de URL (control de filtrado de URL granular, visibilidad de la actividad web del usuario, aplicación de búsquedas seguras y prevención de phishing de credenciales) además de la inspección completa del contenido web mediante un motor de seguridad web basado en aprendizaje automático en línea. El motor de seguridad web en línea permite el análisis en tiempo real y la categorización de las URL que no están presentes en la base de datos de URL basada en la nube de PAN-DB de Palo Alto Networks. Luego, el motor determina la acción que ha de realizar el cortafuegos.

Advanced URL Filtering protege frente a las URL maliciosas que se actualizan o se introducen antes de que PAN-DB las haya analizado y agregado a la base de datos. Con Advanced URL Filtering habilitado, las solicitudes de URL son:

- Analizadas en tiempo real utilizando los módulos de detección de Advanced URL Filtering basados en la nube. Esto se suma a las URL que se comparan con las entradas en PAN-DB. El motor de protección web impulsado por ML detecta y bloquea los sitios web maliciosos que PAN-DB no puede.
- Se realiza una inspección en busca de phishing y JavaScript malicioso mediante la categorización local en línea, una solución de análisis basada en cortafuegos, que puede bloquear páginas web maliciosas desconocidas en tiempo real.

Las licencias Advanced URL Filtering son compatibles con cortafuegos de nueva generación que ejecutan PAN-OS 9.1 y posteriores. Puede gestionar las funciones de filtrado de URL en la interfaz web de PAN-OS y Panorama, en las plataformas Prisma Access y Cloud NGFW. Sin embargo, algunas funciones del filtrado de URL no están disponibles en cada plataforma.

Si los requisitos de seguridad de red en su empresa prohíben que los cortafuegos accedan directamente a Internet, Palo Alto Networks proporciona una solución de filtrado de URL sin conexión con la nube privada de PAN-DB. Puede implementar una nube privada PAN-DB en uno o más dispositivos M-600 que funcionan como servidores PAN-DB dentro de su red; sin embargo, la nube privada no admite ninguna de las características de análisis de URL basadas en la nube que se encuentran en la solución Advanced URL Filtering.

Suscripción de Filtrado de URL heredada

El filtrado de URL aplica las reglas de política para los sitios web almacenados en su caché local o PAN-DB. Cuando un usuario solicita un sitio web, el cortafuegos verifica la caché local para su categoría de URL. Si el sitio web no está en la caché, el cortafuegos consulta PAN-DB para decidir qué acción aplicar. Como resultado, los atacantes pueden lanzar campañas de ataque de precisión utilizando URL que no están presentes en la base de datos basada en la nube.

Los titulares de suscripciones de filtrado de URL heredada pueden seguir utilizando su implementación de filtrado de URL hasta el final del período de licencia.

Compatibilidad con el filtrado de URL

Las funciones de Advanced URL Filtering están disponibles en cortafuegos de nueva generación (virtuales y locales), Prisma Access (Managed by Strata Cloud Manager), Prisma Access (Managed by Panorama), Cloud NGFW para AWS y Cloud NGFW para Azure. Sin embargo, los cortafuegos de nueva generación y Cloud NGFW para Azure requieren una suscripción de Advanced URL Filtering, mientras que todos los Prisma Access y las licencias Cloud NGFW para AWS incluyen capacidades de Advanced URL Filtering.

La compatibilidad de funciones depende de la plataforma y del tipo de licencia de filtrado de URL. Las funciones que solo están disponibles con una licencia de Advanced URL Filtering se indican mediante una etiqueta de Advanced URL Filtering.

La siguiente tabla muestra la compatibilidad de las funciones de Advanced URL Filtering con cada plataforma de Palo Alto Networks que admite URL Filtering.

Función	Compatible con						Notas
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW para AWS	Cloud NGFW para Azure	
Categorización en línea • Categorización en línea local (llamada ML en línea antes de PAN-OS 10.2) • (Advanced URL Filtering) Categorización en línea en la nube	Sí	Sí	Sí	Sí	Sí	Sí	No compatible con el dispositivo VM-50 o VM50L

Función	Compatible con						Notas
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW para AWS	Cloud NGFW para Azure	
Categorías de URL personalizadas	Sí	Sí	Sí	Sí	Sí	Sí	
Detección de credencial de usuario	Sí	Sí	Sí	Sí	Sí	Sí	
Páginas de respuesta de filtrado de URL personalizadas	Sí	Sí	Sí	Sí	Sí	Sí	
Aplicación de búsquedas seguras • Bloquear los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada • Forzar búsqueda segura estricta	Sí	Sí	Sí	Sí	Sí	Sí	

Función	Compatible con						Notas
	NGFW (Managed by Strata Cloud Manager)	NGFW (Managed by PAN-OS or Panorama)	Prisma Access (Managed by Strata Cloud Manager)	Prisma Access (Managed by Panorama)	Cloud NGFW para AWS	Cloud NGFW para Azure	
Cancelación de administrador de URL	Sí	Sí	Sí	Sí	Sí	Sí	
Inspección del protocolo de enlace SSL/TLS	Sí	Sí	Sí	Sí	Sí	Sí	
Integración con el aislamiento remoto del navegador (RBI)	No	No	Sí	Sí	No	No	
Registrar solo la página del contenedor (Registrar solo la página que visita un usuario)	No	Sí	Sí	Sí	Sí	Sí	

Categorización local en línea

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering ***Nota:*** *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

La categorización local en línea (anteriormente conocida como aprendizaje automático en línea) permite que el plano de datos del cortafuegos aplique el aprendizaje automático (ML) en las páginas web para alertar a los usuarios cuando se detectan variantes de phishing y, al mismo tiempo, evita que variantes maliciosas de vulnerabilidades de JavaScript entren en su red. La categorización local en línea analiza y detecta dinámicamente contenidos maliciosos mediante la evaluación de varios detalles de la página web con una serie de modelos de aprendizaje automático. Cada modelo de aprendizaje automático detecta contenido malicioso mediante la evaluación de los detalles del archivo, incluidos los campos y patrones del decodificador, para formular una clasificación y un veredicto de alta probabilidad, que luego se utiliza como parte de su política de seguridad web más amplia. Las URL clasificadas como maliciosas por el se reenvían a PAN-DB para su análisis y validación adicionales. Puede especificar excepciones de URL para excluir cualquier falso positivo que pueda encontrarse. Esto le permite crear reglas más granulares para sus perfiles con el fin de respaldar sus necesidades de seguridad específicas. Para mantenerse al día con los últimos cambios en el entorno de las amenazas, los modelos de aprendizaje automático en línea se actualizan con frecuencia y se añaden mediante lanzamientos de contenido. Se requiere una suscripción activa de Advanced URL Filtering para configurar la categorización en línea.

También se puede eliminar la protección basada en aprendizaje automático en línea para detectar PE maliciosos (portables ejecutables), archivos ELF y MS Office, y scripts de PowerShell y shell en tiempo real como parte de la configuración de su perfil de antivirus. Para obtener más información, consulte: Aprendizaje automático en línea de Advanced WildFire

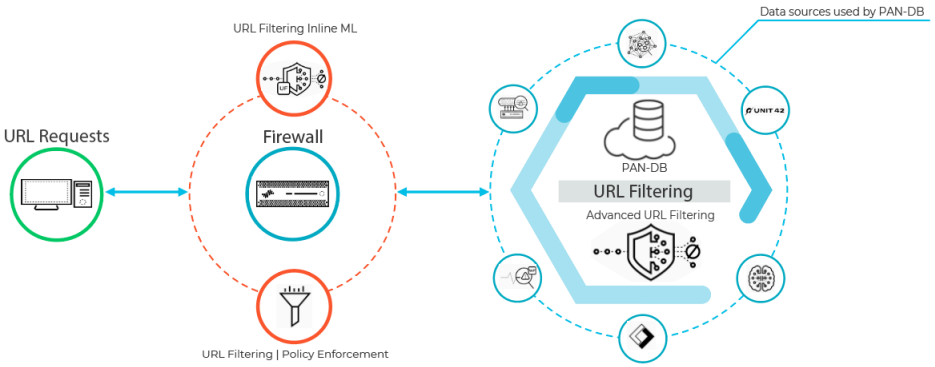
La categorización local en línea no se admite en el dispositivo virtual VM-50 o VM50L.

Cómo funciona Advanced URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Advanced URL Filtering clasifica los sitios web en función del contenido, las características y la seguridad del sitio. Una URL puede tener hasta cuatro categorías de URL que indican la probabilidad de que el sitio lo exponga a amenazas. Como PAN-DB, la base de datos de Advanced URL Filtering, categoriza los sitios, los cortafuegos con el Advanced URL Filtering habilitado pueden aprovechar ese conocimiento para hacer cumplir las políticas de seguridad de su organización. Además de la protección que ofrece PAN-DB, Advanced URL Filtering proporciona análisis en tiempo real mediante aprendizaje automático (ML) para defenderse de amenazas nuevas y desconocidas. Esto proporciona protección contra URL maliciosas que se actualizan o introducen antes de que las bases de datos de filtrado de URL tengan la oportunidad de analizar y añadir el contenido, lo que brinda a los atacantes un período abierto desde el cual pueden iniciar campañas de ataque de precisión. Advanced URL Filtering compensa las brechas de cobertura inherentes a las soluciones de bases de datos gracias a que proporciona análisis de URL en tiempo real a petición. Los modelos basados en ML utilizados por Advanced URL Filtering se han entrenado y se actualizan continuamente para detectar varias URL maliciosas, páginas web de phishing, y comando y control (C2).

Los sitios web que indican la presencia de ciertas amenazas avanzadas también se procesan a través de un sistema de aprendizaje profundo en línea basado en la nube, utilizando detectores y analizadores que complementan los modelos de ML utilizados por Advanced URL Filtering. Los detectores de aprendizaje profundo pueden procesar conjuntos de datos más grandes y pueden identificar mejor patrones y comportamientos maliciosos complejos a través de redes neuronales de múltiples capas. Cuando Advanced URL Filtering recibe datos de respuesta HTTP del cortafuegos al recibir una solicitud web sospechosa, los datos se analizan más a fondo a través de los detectores de aprendizaje profundo y proporcionan protección en línea contra ataques web evasivos de día cero. Esto incluye sitios web encubiertos, en los que el contenido de la página web se recupera subrepticiamente de sitios web desconocidos; esto puede incluir contenido malicioso que las bases de datos de URL no pueden tener en cuenta, ataques de varios pasos, desafíos CAPTCHA y URL de un solo uso nunca antes vistas. Debido a que los sitios web maliciosos evasivos están en un estado constante de flujo, los detectores y analizadores utilizados para categorizar los sitios web se actualizan e implementan automáticamente a medida que los investigadores de amenazas de Palo Alto Networks mejoran la lógica de detección, todo sin requerir que el administrador descargue paquetes de actualización.



Cuando un usuario solicita una página web, el cortafuegos consulta las excepciones agregadas por el usuario y PAN-DB para la categoría de riesgo del sitio. PAN-DB utiliza información de URL de la Unidad 42, WildFire, DNS pasivo, datos de telemetría de Palo Alto Networks, datos de Cyber Threat Alliance y aplica varios analizadores para determinar la categoría. Si la URL muestra características riesgosas o maliciosas, los datos de carga útil web también se envía a Advanced URL Filtering en la nube para su análisis en tiempo real y genera datos de análisis adicionales. A continuación, el cortafuegos recupera la categoría de riesgo resultante y se utiliza para aplicar las reglas de acceso web en función de la configuración de la política. Además, el cortafuegos almacena en caché la información de categorización del sitio para las nuevas entradas a fin de permitir la recuperación rápida de solicitudes posteriores, mientras que elimina las URL a las que los usuarios no han accedido recientemente para que refleje con precisión el tráfico en su red. Además, las comprobaciones integradas en las consultas en la nube de PAN-DB garantizan que el cortafuegos reciba la información de categorización de URL más reciente. Si no tiene conectividad a Internet o una licencia activa de filtrado de URL, no se realizan consultas a PAN-DB.

El cortafuegos determina la categoría de URL de un sitio web comparándola con las entradas de 1) categorías de URL personalizadas, 2) listas dinámicas externas (EDL) y 3) categorías de URL predefinidas, en orden de precedencia.

Los cortafuegos configurados para analizar URL en tiempo real mediante aprendizaje automático en el plano de datos proporcionan una capa adicional de seguridad contra sitios web de phishing y exploits de JavaScript. Los modelos de ML utilizados por la categorización local en línea identifican variantes actualmente desconocidas y futuras de amenazas basadas en URL que coinciden con las características que Palo Alto Networks ha identificado como maliciosas. Para mantenerse al día con los últimos cambios en el panorama de las amenazas, se añaden o actualizan modelos de aprendizaje automático de categorización en línea local a través de lanzamientos de contenido.

Cuando el cortafuegos comprueba una URL en PAN-DB, también busca actualizaciones críticas, como URL que anteriormente se consideraban benignas pero que ahora son maliciosas.

Si cree que PAN-DB ha clasificado incorrectamente un sitio, puede enviar una solicitud de cambio en su navegador a través de Test A Site o directamente desde los logs del cortafuegos.

¿Sabía esto?

Técnicamente, el cortafuegos almacena en caché las URL tanto en el plano de gestión como en el de datos:

- *PAN-OS 9.0 y las versiones posteriores no descargan las bases de datos semilla de PAN-DB. En cambio, tras la activación de la licencia de filtrado de URL, el cortafuegos completa la caché a medida que se realizan consultas de URL.*
- *El plano de gestión contiene más URL y se comunica directamente con PAN-DB. Cuando el cortafuegos no consigue encontrar una categoría de URL en la memoria caché y realiza una búsqueda en PAN-DB, esta almacena en caché la información de la categoría recuperada en el plano de gestión. El plano de gestión pasa esa información al plano de datos, que también la almacena en caché y la usa para aplicar la política.*
- *El plano de datos contiene menos URL y recibe información del plano de gestión. Después de que el cortafuegos verifica las listas de excepciones de categorías de URL (categorías de URL personalizadas y listas dinámicas externas) en busca de una URL, este busca en el plano de datos. Si el cortafuegos no encuentra la URL en el plano de datos, verifica el plano de gestión y, si la información de la categoría no está allí, PAN-DB.*

Perfiles de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Los perfiles de URL Filtering definen cómo el cortafuegos gestiona el tráfico a categorías de URL específicas. Un perfil URL Filtering es un conjunto de controles de filtrado de URL que se aplican a reglas de la política de seguridad individuales para permitir el acceso a Internet. Puede configurar el acceso al sitio para categorías de URL, permitir o no permitir envíos de credenciales de usuario, habilitar la aplicación de búsquedas seguras y otros ajustes. Para hacer cumplir las acciones definidas en un perfil de URL Filtering , aplique el perfil a las reglas de la política de seguridad. El cortafuegos aplica las acciones de perfil en el tráfico que coincide con la regla de la política de seguridad (para obtener más información, consulte Configuración de URL Filtering).

El cortafuegos incluye un perfil predeterminado que bloquea categorías propensas a las amenazas, como malware, phishing y contenido para adultos. Puede utilizar el perfil predeterminado en una regla de la política de seguridad, duplicarlo para utilizarlo como punto de partida para nuevos perfiles de filtrado de URL o añadir un nuevo perfil de URL Filtering. Puede personalizar los perfiles de filtrado de URL recién añadidos y añadir listas de sitios web específicos que siempre deberían bloquearse o permitirse. Por ejemplo, puede bloquear la categoría de redes sociales pero permitir el acceso a sitios web específicos de esa categoría. De manera predeterminada, el acceso al sitio para todas las categorías de URL se configura en permitir cuando crea un nuevo perfil de filtrado de URL. Esto significa que los usuarios podrán navegar por todos los sitios libremente y que el tráfico no se registrará.

Cree un perfil de filtrado de URL recomendado para garantizar la protección frente a las URL que se han observado que alojan malware o contenido que se puede explotar.

Acciones de políticas de perfil de filtrado de URL

En un perfil de filtrado de URL, puede definir el **Site Access (Acceso al sitio)** para las categorías de URL, permitir o no permitir el **User Credential Submissions (Envío de credenciales de usuario)** según la categoría de URL (por ejemplo, puede bloquear las credenciales de usuario enviadas a sitios de riesgo medio y alto) y habilitar la aplicación de búsquedas seguras.

Acción	Description (Descripción)
Acceso a sitio	
alert	El sitio web está permitido y se genera una entrada de log en el log de filtrado de URL. *Configure **alert (Alerta)** como Action (Acción) para las categorías de tráfico que no bloquea registrarse y proporcionar visibilidad en el tráfico.*
allow	El sitio web está permitido y no se genera ninguna entrada de log. *No configure **allow (Permitir)** como Action (Acción) para las categorías de tráfico que no bloquea porque pierde visibilidad en el tráfico que no registra. En cambio, configure **alert (Alerta)** como Action (Acción) para las categorías de tráfico que no bloquea para el registro y proporcionar visibilidad en el tráfico.*
block	El sitio web está bloqueado y el usuario verá una página de respuesta y no podrá ir al sitio web. Se generará una entrada de log en el log de filtrado de URL. El bloqueo del acceso a un sitio para una categoría de URL también establece el bloqueo del envío de credenciales de usuario para esa categoría de URL.
continue	El usuario recibirá una página de respuesta indicando que el sitio se ha bloqueado debido a la política de la empresa, pero se le dará la opción de ir al sitio web. La acción **continue (continuar)** se suele usar para categorías que se consideran inofensivas y se usa para mejorar la experiencia del usuario mediante la posibilidad de continuar si considera que el sitio se ha categorizado incorrectamente. El mensaje de la página de respuesta se puede personalizar para incluir información detallada específica de su empresa. Se generará una entrada de log en el log de filtrado de URL. *La página Continue (Continuar) no se mostrará correctamente en equipos cliente configurados para usar un servidor proxy.*

Acción	Description (Descripción)
override	El usuario verá una página de respuesta indicando que se requiere una contraseña para permitir el acceso a los sitios web de la categoría en cuestión. Con esta opción, el administrador de seguridad o el miembro del servicio de asistencia técnica proporcionarían una contraseña que concedería un acceso temporal a todos los sitios web de la categoría en cuestión. Se generará una entrada de log en el log de filtrado de URL. Consulte Habilitación del acceso a determinados sitios mediante contraseña. En las versiones anteriores, las sustituciones de categorías de URL Filtering tenían prioridad sobre las categorías de URL personalizadas. Como parte de la actualización a PAN-OS 9.0, las sustituciones de categorías de URL se han convertido en categorías de URL personalizadas, y su aplicación ya no tiene prioridad sobre las demás categorías personalizadas. En lugar de aplicar la acción que estaba definida en las versiones anteriores, se aplica la Regla de la política de seguridad que tenga la acción más estricta del perfil de URL Filtering. Las posibles acciones de los perfiles de URL Filtering son, de la más estricta a la menos dura, block (bloquear), override (sustituir), continue (continuar), alert (alertar) y allow (permitir). Por lo tanto, si tenía sustituciones de categorías de URL con la acción allow (permitir), es posible que se bloqueen tras la conversión a la categoría de URL personalizada en PAN-OS 9.0. *La página Override (Cancelar) no se mostrará correctamente en equipos cliente configurados para usar un servidor proxy.*
none	La acción **ninguno** solo se aplica a las categorías de URL personalizadas. Seleccione **none (ninguno)** para asegurarse de que si existen varios perfiles de URL, la categoría personalizada no tendrá ningún efecto en otros perfiles. Por ejemplo, si tiene dos perfiles URL y la categoría URL personalizada está configurada como **block** en un perfil, si no desea que la acción de bloquear se aplique al otro perfil, debe configurar la acción en **none**. Además, para eliminar una categoría de URL personalizada, se debe establecer en **ninguno** en cualquier perfil en el que se use.

Permisos de credenciales de usuario

Acción	Description (Descripción)
Estos ajustes requieren que primero realice la Configuración de la prevención de suplantación de identidad de credenciales.	
alert	Permita a los usuarios que envíen credenciales corporativas a los sitios de esta categoría de URL, pero genere un log de alerta de filtrado de URL cada vez que esto ocurra.
Permitir (opción predeterminada)	Permita a los usuarios que envíen credenciales corporativas a los sitios web de esta categoría de URL.
block	Bloquee a los usuarios para que no envíen credenciales corporativas a los sitios web de esta categoría. La página de respuesta antiphishing predeterminada se muestra a los usuarios cuando acceden a sitios para los cuales los envíos de credenciales corporativas están bloqueados. Puede personalizar la página de bloqueo que se muestra.
continue	Muestra una página de respuesta a los usuarios que solicita que seleccionen Continue (Continuar) para acceder al sitio. De manera predeterminada, la página de continuar para la prevención del phishing se muestra a los usuarios cuando estos ingresan en los sitios para los cuales no se recomienda el envío de credenciales. Puede personalizar la página de respuesta para advertir a los usuarios contra intentos de phishing o reutilización de sus credenciales en otros sitios web, por ejemplo.

Categorías de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Palo Alto Networks clasifica los sitios web según su contenido, características y seguridad. Cada categoría de URL corresponde a un conjunto de características que resultan útiles para crear reglas de políticas. Las URL a las que acceden los usuarios de su red se añaden a la base de datos del filtrado de URL de Palo Alto Networks, PAN-DB. PAN-DB asigna hasta cuatro categorías de URL, incluidas categorías de riesgo (alto, medio y bajo), a estos sitios web.

Las categorías de URL permiten el filtrado basado en categorías del tráfico web y el control granular de las políticas de los sitios. Puede configurar un perfil de URL Filtering para definir el acceso al sitio para categorías de URL y aplicar el perfil a las reglas de la política de seguridad que permiten el tráfico a Internet. También puede utilizar categorías de URL como criterios de coincidencia en las reglas de la política de seguridad para garantizar que dichas reglas se apliquen solo a sitios web en las categorías especificadas. Por ejemplo, puede configurar una regla de política de descifrado que impida el descifrado del tráfico hacia la categoría de servicios financieros.

Para comprobar las categorías de una URL específica, introduzca la URL en Test A Site, nuestro motor de búsqueda de URL. Si cree que una URL está clasificada incorrectamente, envíe una solicitud de cambio de categoría.

Categorías de URL personalizadas

Puede crear una categoría de URL personalizada para excluir sitios web específicos de la aplicación basada en categorías. Las categorías de URL personalizadas pueden basarse en URL específicas (Lista de URL) u otras categorías (Coincidencia de categoría). Las categorías de URL personalizadas del tipo Lista de URL funcionan como listas de bloqueo y de permiso. Las categorías de URL personalizadas del tipo Coincidencia de categoría permiten una imposición específica para sitios web que coinciden con todas las categorías definidas como parte de la categoría personalizada.

Categorías de URL predefinidas

La siguiente tabla enumera las categorías de URL predefinidas que PAN-DB utiliza para filtrar las URL. Algunas entradas describen sitios que están excluidos de la categoría. Categorías de URL centradas en la seguridad describe categorías de riesgo que no están asignadas a todas las URL.

URL Category (Categoría de URL)	Description (Descripción)
Aborto	Sitios que incluyen información o grupos a favor o en contra del aborto, detalles sobre procedimientos de aborto, foros de ayuda o apoyo a favor o en contra del aborto, o sitios que brindan información sobre las consecuencias o efectos de buscar tener (o no) un aborto.
Consumo de drogas	Sitios web que promueven el consumo de drogas legales e ilegales, el uso y venta de parafernalia relacionada con estupefacientes, o la producción o venta de drogas.
Adulto	Sitios con cualquier material, medios (incluyendo lenguaje, juegos o cómics), arte o productos sexualmente explícitos, grupos o foros en línea que sean de naturaleza sexual explícitos y sitios que promuevan servicios para adultos, como videollamadas, servicios de acompañantes y clubes de striptease.
Alcohol y tabaco	Sitios relacionados con la venta, fabricación o consumo de productos alcohólicos o de tabaco, y parafernalia relacionada. Incluye sitios relacionados con los cigarrillos electrónicos.
Inteligencia artificial	Sitios web que utilizan modelos de aprendizaje automático y de aprendizaje profundo, incluidos modelos de lenguaje de gran tamaño, para proporcionar servicios que normalmente habrían requerido inteligencia humana. Los servicios proporcionados incluyen, entre otros, servicios relacionados con la edición de audio o vídeo, chatbot, productividad, resúmenes, transcripciones, sin código. Se da énfasis a los sitios web que albergan el servicio de IA real, no contenido informativo de IA.
Subastas	Sitios que promueven la venta de bienes entre particulares. *Las subastas con fines de donación se clasifican como Sociedad.*
Empresa y economía	Sitios con contenido relacionado con marketing, gestión, economía, emprendimiento o gestión de empresas, incluidos los siguientes: • Sitios para empresas de publicidad y marketing

URL Category (Categoría de URL)	Description (Descripción)
	• Sitios para servicios de mensajería, como fedex.com • Sitios para proveedores de servicios de telefonía, cable e Internet • Sitios para encuestas o sondeos • Sitios para Cámaras de comercio • Sitios para congresos* • *Los sitios web corporativos podrían clasificarse según su tecnología en lugar de esta categoría.* • ** Los sitios relacionados con congresos deben clasificarse según el contenido. Si el contenido de un sitio no es específico, se clasifica como Empresa y economía.*
Comando y control	URL y dominios de comando y control (C2) utilizados por malware o sistemas comprometidos para comunicarse de manera furtiva con el servidor remoto de un atacante para recibir comandos maliciosos o exfiltrar datos.
Información de informática e Internet	Sitios que proporcionan información general sobre equipos informáticos e Internet, incluidos sitios sobre los siguientes temas: • Informática • Ingeniería • Hardware y componentes de equipos informáticos • Software • Seguridad • Programación *La Programación puede tener cierta superposición con la categoría de Referencia e investigación, pero la categoría principal debería ser Información sobre equipos informáticos e Internet.*

URL Category (Categoría de URL)	Description (Descripción)
Redes de entrega de contenido	Sitios cuyo objetivo principal es entregar contenido a terceros, por ejemplo servidores de anuncios, medios, archivos e imágenes.
Violación de copyright	Dominios con contenido ilegal, como contenido que permite la descarga ilegal de software u otra propiedad intelectual, lo que representa un riesgo potencial de responsabilidad. *Los sitios que proporcionan servicios de intercambio de archivos entre pares o transmisión multimedia en general pertenecen a sus respectivas categorías.*
criptomonedas	Sitios que promueven criptomonedas, sitios de criptominería (pero no mineros de criptomonedas integrados), intercambios y proveedores de criptomonedas, y sitios que gestionan billeteras y cuentas de criptomonedas. *Los sitios que hacen referencia a criptomonedas o sitios maliciosos relacionados con criptomonedas se clasificarán por separado. Por ejemplo, los sitios que explican cómo funcionan las criptomonedas y la tecnología blockchain se incluyen en Información de informática e Internet.*
Citas	Sitios que ofrecen servicios de citas en línea, consejos u otros anuncios personales. *Los sitios de citas que ofrecen salas de chat sobre sexo entran en la categoría de adultos.*
DNS dinámico	Sitios que proporcionan o utilizan servicios de DNS dinámicos para asociar nombres de dominio con direcciones IP dinámicas. *Los atacantes suelen utilizar DNS dinámicos para comunicaciones de comando y control, y otros fines maliciosos.*

URL Category (Categoría de URL)	Description (Descripción)
Instituciones académicas	Sitios oficiales de escuelas, instituciones de educación superior, universidades, distritos escolares, clases en línea y otras instituciones académicas. También incluye sitios para centros de apoyo escolar. *Esta categoría hace referencia a instituciones académicas más grandes y establecidas, como colegios de primaria, institutos de secundaria y universidades.*
DNS cifrado	Sitios para proveedores de servicios de resolución de DNS, que ofrecen seguridad y privacidad a los usuarios finales al cifrar las solicitudes y respuestas de DNS utilizando protocolos como DNS sobre HTTPS (DoH).
Arte y entretenimiento	Sitios de películas, televisión, radio, vídeos, guías o herramientas de programación, cómics, artes escénicas, museos, galerías de arte o bibliotecas. Incluye sitios para lo siguiente: • Entretenimiento • Noticias sobre celebridades y la industria del entretenimiento • Novelas • Clases de baile • Lugares para eventos • Arte del tatuaje
Extremismo	Sitios web que promuevan el terrorismo, el racismo, el fascismo u otras opiniones que discriminen a personas o grupos de diferentes orígenes étnicos, religiones u otras creencias. En algunas regiones, la legislación y las normativas prohíben que se permita el acceso a sitios extremistas, lo que puede acarrear una responsabilidad civil. *Los sitios web que debaten opiniones políticas o religiosas controvertidas se incluyen en las categorías de Filosofía y defensa política y Religión, respectivamente.*
Servicios financieros	Sitios relacionados con finanzas personales o asesoramiento, como banca en línea, préstamos,

URL Category (Categoría de URL)	Description (Descripción)
	hipotecas, gestión de deudas, empresas de tarjetas de crédito, casas de cambio (FOREX) y empresas aseguradoras. Se excluyen sitios relacionados con seguros de salud, mercados de valores, empresas de inversión o servicios de intermediación.
Juegos de azar	Sitios que facilitan el intercambio de dinero real o virtual a través de loterías o juegos de azar. Incluye sitios relacionados que brindan información, tutoriales o consejos sobre juegos de azar, como por ejemplo cómo apostar en cuotas y porras. *Los sitios web corporativos de hoteles y casinos que no permiten juegos de azar entran en la categoría de Viajes.*
Juegos	Sitios que ofrecen juegos en línea o descargas de vídeos o juegos de ordenador, reseñas de juegos, consejos, trucos o publicaciones y medios relacionados. Incluye sitios que proporcionan instrucciones para juegos no electrónicos, facilitan la venta o el intercambio de juegos de mesa, o apoyan u organizan sorteos y obsequios en línea.
Gobierno	Sitios web oficiales de gobiernos locales, regionales y estatales; así como agencias, servicios o legislación relacionados. *Los sitios web de bibliotecas públicas e instituciones militares se incluyen en las categorías de Referencia e Investigación y Militar, respectivamente.*
Grayware	Sitios con contenido que no representa una amenaza directa a la seguridad pero que muestra otro comportamiento intrusivo y que tienta a los usuarios finales a proporcionar acceso remoto o realizar otras acciones no autorizadas. El grayware incluye lo siguiente: • Sitios hackeados • Dominios con errores tipográficos deliberados que no muestran un comportamiento malicioso y que no son propiedad del dominio en cuestión • Sitios con rogueware, adware u otras aplicaciones no solicitadas, como criptomineros integrados,

URL Category (Categoría de URL)	Description (Descripción)
	secuestradores de clics o secuestradores que modifican los elementos del navegador web • Sitios con contenido relacionado con actividades ilegales o delictivas
Hackear	Sitios relacionados con el acceso o uso ilegal o cuestionable de equipos o software de comunicaciones, incluido el desarrollo y la distribución de dichos programas, consejos prácticos o sugerencias que puedan resultar en riesgos para redes y sistemas. Incluye sitios que facilitan evitar los sistemas de licencias y derechos digitales.
Salud y medicina	Sitios que contienen información sobre salud general, problemas y consejos, remedios y tratamientos tradicionales y no tradicionales. Incluye sitios para diversas especialidades médicas, consultas, instalaciones (como gimnasios y clubes de fitness) y profesionales. También se incluyen sitios relacionados con seguros médicos y cirugía estética.
Casa y jardín	Sitios web con información, productos y servicios relacionados con la reparación y mantenimiento del hogar, arquitectura, diseño, construcción, decoración y jardinería.
Caza y pesca	Sitios web que ofrecen consejos o instrucciones de caza y pesca, o facilitan la venta de equipos y parafernalia relacionados. *Los sitios web que venden principalmente armas de fuego (incluso si se utilizan para cazar) entran en la categoría de Armas.*
Contenido insuficiente	Sitios y servicios que presentan páginas de prueba, no tienen contenido, proporcionan acceso a la API que los usuarios finales no tienen que ver o requieren autenticación sin mostrar ningún otro contenido que sugiera una categorización diferente.
Comunicaciones por internet y telefonía	Sitios compatibles o que proporcionan servicios de vídeo chat, mensajería instantánea u otras capacidades de telefonía.

URL Category (Categoría de URL)	Description (Descripción)
Portales de Internet	Sitios que sirven como punto de partida para los usuarios, generalmente mediante la suma de un conjunto amplio de contenidos y temas.
Búsqueda de trabajo	Sitios que ofrecen listados de trabajos, reseñas de empleadores, consejos y sugerencias para entrevistas o servicios relacionados tanto para empleadores como para posibles candidatos.
Legal	Sitios web que brindan información, análisis o asesoramiento sobre leyes, servicios jurídicos, despachos jurídicos u otros temas relacionados con el derecho.
Malware	Sitios que contienen o se sabe que albergan contenido malicioso, ejecutables, scripts, virus, troyanos y códigos.
Marihuana	Sitios que discuten, alientan, promueven, ofrecen, venden, suministran o de otra manera defienden el uso, cultivo, producción o distribución de marihuana y sus innumerables alias, ya sea con fines recreativos o medicinales. Incluye sitios con contenido sobre parafernalia relacionada con la marihuana.
Militar	Sitios con información o comentarios sobre ramas militares, reclutamiento, operaciones actuales o pasadas o cualquier parafernalia relacionada. Incluye sitios web para asociaciones militares y de veteranos.
Vehículos de motor	Sitios con información relacionada con revisiones, ventas, intercambios, modificaciones, repuestos y otras discusiones relacionadas con automóviles, motocicletas, barcos, camiones y vehículos recreativos (RV).
Música	Sitios web relacionados con la venta, distribución o información de música. Incluye sitios web para artistas musicales, grupos, sellos, eventos, letras y otra información relacionada con el negocio de la música. Excluye sitios web de streaming de música.
Dominios recién registrados	Sitios web que se han registrado en los últimos 32 días. A menudo, los dominios recién registrados se generan a propósito o mediante algoritmos de generación de dominios y pueden usarse para actividades maliciosas.

URL Category (Categoría de URL)	Description (Descripción)
Noticias	Publicaciones en línea, servicios de noticias y otros sitios web que agregan eventos actuales, clima u otros temas contemporáneos. Incluye los siguientes: • Periódicos • Estaciones de radio • Revistas • Podcasts • Programas de televisión dedicados a las noticias. • Sitios de marcadores sociales, como reddit.com *Si la revista o el sitio web de noticias se centra en un tema específico, como deportes, viajes o moda, esta se clasifica según el contenido dominante en el sitio.*
Sin resolver	Esta categoría indica que no se encontró el sitio web en la base de datos de filtrado de URL local y el cortafuegos no pudo conectarse a la base de datos en la nube para verificar la categoría.
Desnudez	Sitios que contienen representaciones de desnudos o semidesnudos, independientemente del contexto o la intención, como obras de arte. Incluye sitios nudistas o naturistas que contienen imágenes de los participantes.
Almacenamiento y copia de seguridad en línea	Sitios que ofrecen almacenamiento de archivos en línea de forma gratuita o como servicio. Incluye sitios para compartir fotografías.
Estacionado	URL que alojan contenido limitado o anuncios de porcentaje de clics, que pueden generar ingresos para la entidad anfitriona, pero que generalmente no contienen contenido que sea útil para los usuarios finales. Incluye dominios que están a la venta. *Los sitios estacionados con contenido para adultos entran en la categoría Adultos.*
Peer-to-peer	Sitios que proporcionan acceso a o clientes para compartir, peer-to-peer, programas de descarga, archivos multimedia u otras aplicaciones de software. Se aplica principalmente a aquellos sitios con

URL Category (Categoría de URL)	Description (Descripción)
	capacidades de descarga tipo BitTorrent. Excluye sitios de shareware o freeware.
Sitios personales y blogs	Sitios web y blogs personales de individuos o grupos. Si dichos sitios tienen un tema dominante asociado con otra categoría, se clasificarán con ambas categorías.
Filosofía y defensa política	Sitios que contienen información, puntos de vista o campañas relacionadas con opiniones filosóficas o políticas.
Phishing	Contenido web que intenta de forma encubierta recopilar información, como credenciales de inicio de sesión, información de tarjetas de crédito, números de cuenta, PIN y otra información de identificación personal (PII), de forma voluntaria o involuntaria, de las víctimas mediante técnicas de ingeniería social. Incluye estafas de soporte técnico y scareware.
Direcciones IP privadas	Esta categoría incluye direcciones IP definidas en RFC 1918, 'Asignación de direcciones para intranets privadas', que son las siguientes: • 10.0.0.0 - 10.255.255.255 (prefijo 10/8) • 172.16.0.0 - 172.31.255.255 (prefijo 172.16/12) • 192.168.0.0 - 192.168.255.255 (prefijo 192.168/16) Incluye dominios no registrados en el sistema de DNS pública (como *.local y *.onion).
Evasión de proxy y anonimizadores	Servidores proxy y otros métodos que evitan el filtrado o la supervisión de URL. *Las VPN con uso a nivel corporativo entran en la categoría de Comunicaciones por Internet y telefonía.*
Cuestionable	Sitios web que contienen humor de mal gusto o contenido ofensivo dirigido a grupos demográficos específicos de individuos o personas.
Ransomware	Sitios conocidos por albergar ransomware o tráfico malicioso involucrado en la realización de campañas de ransomware que generalmente amenazan con publicar datos privados o mantener bloqueado el

URL Category (Categoría de URL)	Description (Descripción)
	acceso a datos o sistemas específicos, generalmente cifrándolos hasta que se pague el rescate exigido. Incluye URL que entregan stealers, wipers y loaders relacionados que pueden contener cargas útiles de ransomware.
Inmobiliaria	Sitios que brindan información sobre alquileres y ventas de propiedades y consejos o información relacionada, incluidos sitios para lo siguiente: • Empresas y agentes inmobiliarios • Servicios de alquiler • Listados (y agregados) • Empresas de reformas • Asociaciones de propietarios • Grupos o individuos de administración de fincas *Los sitios para proveedores de servicios de hipotecas y préstamos se incluyen en la categoría de Servicios Financieros.*
Detección en tiempo real (sólo Advanced URL Filtering)	URL que se han analizado y detectado mediante análisis en línea en tiempo real como parte del Advanced URL Filtering.
Recreación y hobbies	Sitios que consisten en información, foros, asociaciones, grupos o publicaciones relacionadas con actividades recreativas y pasatiempos. *Los sitios que venden productos relacionados con actividades recreativas o pasatiempos, como REI.com, entran en la categoría de Compras.*
Referencia e investigación	Sitios que proporcionan portales, materiales o servicios de referencia personal, profesional o académica, incluidos diccionarios en línea, mapas, almanaques, información censal, bibliotecas, genealogía e información científica. Incluye sitios para o relacionados con lo siguiente: • Páginas Amarillas • Calendario • Bibliotecas públicas • Instituciones de investigación

URL Category (Categoría de URL)	Description (Descripción)
	• Servicios de seguimiento de vehículos ligeros • Documentos y registros relacionados con bienes inmuebles, tráfico, etc. (aún cuando pertenezcan al gobierno)
Religión	Sitios con información sobre diversas religiones, actividades relacionadas o eventos. Incluye sitios para organizaciones religiosas, autoridades religiosas, lugares de culto, adivinación, astrología, horóscopos y parafernalia religiosa. *Los sitios de escuelas primarias o secundarias privadas afiliadas a una organización religiosa, como escuelas católicas, con un plan de estudios que enseña educación religiosa y asignaturas seculares, se incluyen en la categoría de Instituciones académicas*
Actividad de escaneo (solo Advanced URL Filtering)	Campañas llevadas a cabo por adversarios que pueden ser indicadores de riesgo o intentos de realizar ataques dirigidos o investigar vulnerabilidades existentes. Por lo general, estas son parte de una actividad de reconocimiento realizada por los adversarios.
Motores de búsqueda	Sitios que proporcionan una interfaz de búsqueda utilizando palabras clave, frases u otros parámetros que pueden devolver información, sitios web, imágenes u otros archivos como resultados.
Educación sexual	Sitios que proporcionan información sobre reproducción, desarrollo sexual, prácticas sexuales seguras, enfermedades de transmisión sexual, control de la natalidad, consejos para un mejor sexo, y cualquier producto o parafernalia relacionada. Incluye sitios para grupos, foros u organizaciones relacionados.
Shareware y Freeware	Sitios que brindan acceso a software, protectores de pantalla, iconos, fondos de pantalla, utilidades, tonos de llamada, temas o widgets de forma gratuita o mediante donaciones. Incluye proyectos de código abierto.
Compras	Sitios que facilitan la compra de bienes y servicios. Incluye comerciantes en línea, sitios para grandes

URL Category (Categoría de URL)	Description (Descripción)
	superficies, tiendas minoristas, catálogos y herramientas de agregación o supervisión de precios. Los sitios de esta categoría deben ser comerciantes en línea que vendan una variedad de artículos (o cuyo propósito principal sean las ventas online). *Un sitio web de una empresa de cosméticos que permite compras en línea pertenece a la categoría de Cosméticos.*
Redes sociales	Comunidades de usuarios o sitios donde los usuarios interactúan entre sí, publican mensajes, imágenes y se comunican de otro modo con grupos de personas. *Los sitios personales, blogs o foros se incluyen en la categoría Sitios y blogs personales.*
Sociedad	Sitios con contenido relacionado con la población en general o temas que impactan a una gran variedad de personas, como moda, belleza, grupos filantrópicos, sociedades o los niños. Incluye sitios web de restaurantes. *Los sitios web corporativos relacionados con la alimentación, como Burger King, entran en la categoría de Empresa y economía.*
Deportes	Sitios con información sobre eventos deportivos, deportistas, entrenadores, oficiales, equipos u organizaciones, puntuaciones, horarios, noticias relacionadas o parafernalia deportiva. Incluye sitios web para deportes de fantasía y ligas deportivas virtuales. *Los sitios cuyo objetivo principal es vender artículos deportivos entran en la categoría de Compras.*
Consejos sobre acciones y herramientas	Sitios con información sobre el mercado de valores, negociación de acciones u opciones, gestión de carteras, estrategias de inversión, cotizaciones o noticias relacionadas.

URL Category (Categoría de URL)	Description (Descripción)
Transmisión de medios	Sitios que transmiten contenido de audio o vídeo de forma gratuita o mediante pago, incluidas estaciones de radio en línea, servicios de streaming de música y el archivado de podcasts.
Bañadores y lencería	Sitios que incluyen información o imágenes sobre bañadores, ropa íntima u otra vestimenta sugerente.
Entrenamiento y herramientas	Sitios que ofrecen educación, formación y materiales relacionados en línea. Incluye autoescuelas, formación en el trabajo, juegos, aplicaciones, herramientas con fines educativos y academias que proporcionan tutorías. *Las clases de habilidades específicas se clasifican según su tema. Por ejemplo, los sitios web para clases de música entran en la categoría Música.*
Traducción	Sitios que ofrecen servicios de traducción, incluidas entradas de usuario y traducciones de la URL. Estos sitios también pueden permitir a los usuarios eludir el filtrado, ya que el contenido de la página de destino se presenta dentro del contexto de la URL del traductor.
Viajes	Sitios que brindan información sobre viajes, como consejos, ofertas, precios, información de destinos, turismo y servicios relacionados, como herramientas de reserva o supervisión de precios. Incluye sitios web para lo siguiente: • Atracciones locales • Hoteles • Aerolíneas • Empresas de cruceros • Casinos (si el sitio no permite juegos de azar en línea) • Agencias de viajes • Alquiler de vehículos • Instalaciones de aparcamiento
Desconocido	Sitios que Palo Alto Networks aún no ha identificado.

URL Category (Categoría de URL)	Description (Descripción)
	Si la disponibilidad de este sitio es vital para la empresa y debe permitir el tráfico, avise sobre los sitios desconocidos, aplique al tráfico los perfiles recomendados de seguridad e investigue las alertas. *Las actualizaciones en tiempo real de PAN-DB memorizan sitios desconocidos después de un primer intento de acceder a estos sitios, por lo que las URL desconocidas se identifican rápidamente y se convierten en URL conocidas que el cortafuegos puede gestionar en función de la categoría de URL real.*
Armas	Sitios que gestionan ventas u ofrecen reseñas, descripciones o instrucciones sobre armas, armaduras, chalecos antibalas y su uso. *Los sitios relacionados con el tiro al plato, campos de tiro y tiro con arco reciben la categoría principal de Armas y una categoría secundaria de Deportes.*
Anuncios web	Sitios con anuncios, medios, contenido y banners. Incluye páginas para suscribirse y darse de baja de boletines informativos o anuncios.
Correo electrónico basado en web	Cualquier sitio web que proporcione acceso a una bandeja de entrada de correo electrónico y la capacidad de enviar y recibir correos electrónicos. Se da énfasis a los sitios web que ofrecen acceso público gratuito o de pago a dichos servicios.
Alojamiento web	Sitios que ofrecen servicios de alojamiento gratuitos o de pago para páginas web. Incluye sitios con información sobre desarrollo web, publicación, promoción y otros métodos para aumentar el tráfico.

Categorías de URL centradas en la seguridad

PAN-DB evalúa y asigna automáticamente una categoría de riesgo (`riesgo alto`, `riesgo medio`y `riesgo bajo`) a las URL que *no* ha clasificado como maliciosas o que *ya no* clasifica como maliciosas porque han mostrado solo actividad benigna durante al menos 30 días. Cada categoría de riesgo tiene criterios específicos que deben cumplirse para que una URL reciba una categoría determinada. A medida que cambia el contenido del sitio, la categoría de riesgo y la aplicación de políticas se adaptan dinámicamente.

Si PAN-DB determina que una URL pertenece a una categoría de URL maliciosa, no asigna al sitio una categoría de riesgo. En cambio, el cortafuegos bloquea automáticamente el sitio porque representa un riesgo inaceptable para la mayoría de los entornos.

Las direcciones IP privadas (y los hosts) son exclusivos del entorno del host y son invisibles para PAN-DB. Como resultado, Palo Alto Networks no asigna una calificación de riesgo a los sitios en esta categoría.

Las categorías de URL centradas en la seguridad facilitan el descifrado específico y la aplicación de políticas, lo que ayuda a reducir la superficie de ataque. Por ejemplo, puede bloquear el acceso de los usuarios a sitios web de riesgo alto y medio y a dominios recientemente registrados, o descifrar el tráfico a estas categorías si decide permitirlos.

La siguiente tabla enumera descripciones y acciones de políticas predeterminadas y recomendadas para cada categoría de riesgo.

No puede enviar solicitudes para modificar las categorías de URL centradas en la seguridad.

URL Category (Categoría de URL)	Description (Descripción)
Riesgo alto	• Sitios cuyo dominio ha identificado el modelo ML como poseedor de propiedades previamente vinculadas a dominios maliciosos conocidos o que tenían señales de baja reputación web. • Sitios previamente confirmados como sitios de malware, phishing o de comando y control (C2). • Sitios asociados con actividades maliciosas confirmadas o que comparten un dominio con un sitio que se sabe que es malicioso. • Sitios alojados con proveedores de servicios de internet (internet service provider, ISP) blindados. • Dominios clasificados como DDNS debido a la presencia de una configuración DNS dinámica activa. • Sitios alojados en direcciones IP de números de sistemas autónomos (autonomous system number, ASN) conocidos por permitir contenido malintencionado. • Sitio clasificado como *desconocido*. *Estos sitios seguirán siendo de alto riesgo hasta que PAN-DB complete el análisis y la categorización del sitio.*

URL Category (Categoría de URL)	Description (Descripción)
	• Los sitios permanecen en esta categoría durante al menos 30 días. **Acción de la política predeterminada y recomendada: Alerta**
Riesgo medio	• Sitios que se habían confirmado como de malware, de phishing o de comando y control (command-and-control, C2), pero que solo han mostrado actividad benigna durante al menos 30 días. • Todos los sitios de almacenamiento en la nube (sitios clasificados como de *almacenamiento y copia de seguridad en línea*). • Direcciones IP clasificadas como *desconocidas*. *Estas direcciones IP seguirán siendo de riesgo medio hasta que PAN-DB complete el análisis y la categorización del sitio.* • Los sitios permanecen en esta categoría durante 60 días más. **Acción de la política predeterminada y recomendada: Alerta**
Riesgo bajo	Sitios que no conllevan un riesgo medio ni alto. Estos sitios han mostrado actividad benigna durante un mínimo de 90 días. **Acción de la política predeterminada y recomendada: Permitir**
Dominios recién registrados	Identifica los sitios que se han registrado en los 32 últimos días. Es frecuente que las campañas malintencionadas utilicen los dominios nuevos como herramientas. *A menudo, los dominios recién registrados se generan a propósito o con algoritmos de generación de dominios para destinarlos a actividades malintencionadas. Es una práctica recomendada bloquear esta categoría de URL.* **Acción de la política predeterminada: Alerta** **Acción de la política recomendada: Bloquear**

Categorías de URL maliciosas

Le recomendamos encarecidamente que bloquee las siguientes categorías de URL dado que identifican contenido y comportamiento malicioso o intrusivo.

- **Mando y control**
- **violación de copyright**
- **dns dinámico**
- **extremismo**
- **grayware**
- **malware**
- **dominio recién registrado**
- **estacionado**
- **phishing**
- **evasión de proxy y anonimizadores**
- **cuestionable**
- **ransomware**
- **actividad de escaneo**
- **unknown**

Para las categorías sobre las que alerta, en lugar de bloquearlas, puede controlar estrictamente cómo interactúan los usuarios con el contenido del sitio. Por ejemplo, franquee a los usuarios el acceso a los recursos que necesitan (como blogs de desarrolladores con fines de investigación o servicios de almacenamiento en la nube), pero adopte las siguientes medidas de precaución para reducir la exposición a las amenazas web:

- Siga las prácticas recomendadas antispyware, de protección frente a vulnerabilidades y de bloqueo de archivos. Una posible medida de protección consiste en impedir la descarga de tipos de archivos peligrosos y código JavaScript oculto de los sitios sobre los que se notifican alertas.
- Elija los objetivos del descifrado en función de las categorías de URL. Un buen punto de partida es descifrar los sitios de alto y medio riesgo.
- Muestre una página de respuesta a los usuarios cuando visiten sitios de riesgo medio y alto. Avíseles de que el sitio al que quieren acceder puede ser malintencionado y, si aún desean visitarlo, aconséjeles medidas de precaución.
- Evite el phishing de credenciales mediante el bloqueo de los usuarios para que no envíen sus credenciales corporativas a sitios, incluidos aquellos de alto y medio riesgo.

La siguiente tabla enumera las categorías que PAN-DB considera maliciosas y bloquea de forma predeterminada, excepto las `direcciones IP privadas`. Las direcciones IP privadas (y los hosts) son exclusivos del entorno del host y son invisibles para PAN-DB. Como resultado, Palo Alto Networks no asigna una calificación de riesgo a los sitios en esta categoría.

Category	Acción predeterminada
Comando y control	Bloquear
Grayware	
Malware	
Phishing	
Ransomware	
Actividad de escaneo	
Direcciones IP privadas	Allowed (Permitido) (sin acción predeterminada)

Casos de uso de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Hay muchas maneras de hacer cumplir el acceso a la página web más allá de solo bloquear y permitir ciertos sitios. Por ejemplo, puede usar varias categorías por URL para permitir a los usuarios acceder a un sitio, pero bloquear funciones concretas como enviar credenciales corporativas o descargar archivos. También puede usar categorías de URL para aplicar diferentes tipos de política, como Authentication (Autenticación), Decryption (Descifrado), QoS y Security (Seguridad).

Siga leyendo para obtener más información sobre las diferentes formas en que puede implementar el filtrado de URL.

Control del acceso web según la categoría de URL

Puede crear un perfil de URL Filtering que especifica una acción para una categoría de URL y adjunta el perfil a una regla de la política de seguridad. El cortafuegos aplica la política en el tráfico en función de la configuración del perfil. Por ejemplo, para bloquear todos los sitios web de juegos, configuraría la acción de bloqueo para la categoría *juegos* en un perfil de filtrado de URL. Después, adjuntaría el perfil a las reglas de la política de seguridad que permiten el acceso web.

Filtrado de URL de varias categorías

Cada URL puede tener hasta cuatro categorías, incluida una categoría de riesgo que indica la probabilidad con que un sitio suponga una amenaza. Las categorizaciones de URL más detalladas le permiten ir más allá de un enfoque básico de "bloquear o permitir" para el acceso web. En cambio, puede controlar cómo sus usuarios interactúan con contenido en línea que, aunque es necesario para la empresa, es más probable que se use como parte de un ciberataque.

Por ejemplo, puede considerar que determinadas categorías de URL suponen un riesgo para su empresa, pero duda en bloquearlas directamente, ya que también proporcionan recursos o servicios valiosos (como servicios de almacenamiento en la nube o blogs). Ahora puede permitir que los usuarios visiten sitios que se encuentren en estos tipos de categorías mientras descifra e inspecciona el tráfico, y aplica el acceso de solo lectura al contenido.

También puede definir una categoría de URL personalizada seleccionando **Category Match (Coincidencia de categorías)** y especificando dos o más categorías pan-DB de las que constará la nueva categoría. La creación de una categoría personalizada a partir de varias categorías le

permite orientar la aplicación de un sitio web o una página que coincida con todas las categorías especificadas en el objeto de categoría de dirección URL personalizada.

Permiso o bloqueo de envíos de credenciales corporativas según la categoría de URL

Prevenga el phishing de credenciales mediante la habilitación del cortafuegos, la detección de envíos de credenciales corporativas a los sitios y el control de esos envíos según la categoría de URL. Bloquee a los usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre el ingreso de credenciales corporativas en sitios desconocidos o la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos y aprobados.

Aplicación de la configuración de búsqueda segura

Muchos motores de búsqueda incluyen una opción de búsqueda segura que filtra las imágenes y los vídeos para adultos de los resultados de búsqueda. Puede habilitar el cortafuegos para bloquear los resultados de búsqueda o habilitar de forma transparente la búsqueda segura para los usuarios finales que no utilizan la configuración de búsqueda segura más estricta. El cortafuegos admite la aplicación de búsqueda segura para los siguientes proveedores de búsquedas: Google, Yahoo, Bing, Yandex y YouTube. Consulte cómo comenzar con Aplicación de búsquedas seguras.

Aplicación del acceso a determinados sitios mediante contraseña

Puede bloquear el acceso a un sitio para la mayoría de los usuarios y permitir que determinados usuarios accedan al sitio. Consulte cómo permitir el acceso a determinados sitios mediante contraseña.

Bloqueo de descargas de archivos de alto riesgo de determinadas categorías de URL

Puede bloquear las descargas de archivos de alto riesgo de categorías de URL específicas mediante la creación de una regla de la política de seguridad con un Perfil de bloqueo de archivos adjunto.

Aplicación de políticas de seguridad, descifrado, autenticación y QoS basadas en la categoría de URL

Puede aplicar diferentes tipos de políticas de cortafuegos según las categorías de URL. Por ejemplo, suponga que ha habilitado descifrado, pero desea evitar que se descifre determinada información personal. En ese caso, podría crear una regla de políticas de descifrado que excluya los sitios web que coincidan con las categorías de URL *servicios financieros* y *salud y medicina* del descifrado. Otro ejemplo sería utilizar la categoría de URL *aplicaciones de transmisión multimedia* en una política de QoS para aplicar controles de ancho de banda a los sitios web que forman parte de esta categoría.

La siguiente tabla describe las políticas que aceptan las categorías de URL como criterios de coincidencia:

Tipo de política	Description (Descripción)
descifrado	También puede usar categorías de URL para descifrar gradualmente y excluir categorías de URL que puedan contener información confidencial o personal del

Tipo de política	Description (Descripción)
	descifrado (como servicios financieros y salud y medicina). Planifique descifrar primero el tráfico más peligroso (las categorías de URL con mayor probabilidad de tener tráfico malicioso, como los juegos o de alto riesgo) y luego, descifre más a medida que gane experiencia. Como alternativa, descifre primero las categorías de URL que no afecten a su empresa (si algo no funciona, no afectará a la empresa), por ejemplo, las fuentes de noticias. En ambos casos, descifre algunas categorías de URL, escuche los comentarios del usuario, ejecute informes para garantizar que el descifrado funciona según lo esperado y, luego, descifre de manera gradual algunas categorías de URL más y así sucesivamente. Planifique realizar exclusiones de descifrado para excluir sitios del descifrado si no puede descifrarlos por motivos técnicos o porque decide no hacerlo. *Se recomienda descifrar el tráfico según las categorías de URL tanto para el filtrado de URL como para el descifrado.*
Autenticación	Para garantizar que los usuarios están autenticados antes de permitirles el acceso a una categoría específica, puede adjuntar una categoría de URL como criterio de coincidencia para las reglas de la política de autenticación.
QoS	Utilizan categorías de URL para asignar los niveles de rendimiento de categorías específicas de sitios web. Por ejemplo, puede que quiera permitir la categoría *aplicaciones de transmisión multimedia* y al mismo tiempo limitar el rendimiento añadiendo la categoría de URL a la regla políticas de QoS.
Seguridad	Puede utilizar una categoría de URL como criterio de coincidencia o crear un Perfil de URL Filtering que especifica una acción para cada categoría y la asocia a una regla de la política de seguridad.

Tipo de política	Description (Descripción)

	 ***Uso de categorías de URL como criterios de coincidencia frente a aplicación de un perfil de filtrado de URL a una regla de la política de seguridad***
	• *Utilice las categorías de URL como criterios de coincidencia en los siguientes casos:*
	  • *Para crear una excepción a la aplicación de categorías de URL*
	  • *Para asignar una acción concreta a una categoría de URL personalizada o predefinida. Por ejemplo, puede crear una regla de la política de seguridad que permita el acceso a sitios en la categoría Sitios personales y blogs.*
	• *Utilice un perfil de filtrado de URL en los siguientes casos:*
	  • *Para registrar el tráfico a categorías de URL en los logs de filtrado de URL*
	  • *Para especificar acciones más granulares, como alertas, en el tráfico para una categoría específica*
	  • *Para configurar una página de respuesta que se muestra cuando los usuarios acceden a un sitio web bloqueado o bloqueado-continuar.*
	En un perfil de filtrado de URL, las acciones especificadas para cada categoría de URL solo se aplican al tráfico destinado a las categorías especificadas en la regla de la política de seguridad. También puede aplicar un perfil determinado a varias reglas.

Tipo de política	Description (Descripción)
	Si, por ejemplo, el grupo de seguridad de TI de su empresa necesita acceder a la categoría *hacking*, pero a todos los demás usuarios se les deniega el acceso a la categoría, deberá crear las siguientes reglas: • Una regla de la política de seguridad que permita que el grupo seguridad de TI acceda al contenido categorizado como *hacking*. La regla de la política de seguridad hace referencia a la categoría *hacking* de la pestaña **Services/URL Category (Servicio/Categoría de URL)** y el grupo de seguridad de TI en la pestaña **Users (Usuarios)**. • Otra regla de la política de seguridad que permita acceso web general a todos los usuarios. Para esta regla, adjunte un perfil de filtrado de URL que bloquea la categoría *hackeo*. Debe indicar la política que permite el acceso al *hacking* antes de la política que bloquea el *hacking*. Esto se debe a que el cortafuegos evalúa las reglas de la política de seguridad de arriba hacia abajo, por lo que cuando un usuario que forma parte del grupo de seguridad intenta acceder a un sitio de *hacking*, el cortafuegos evalúa primero la regla de políticas que permite el acceso y otorga acceso al usuario. El cortafuegos evalúa los usuarios de todos los demás grupos con respecto a la regla general de acceso web que bloquea el acceso a los sitios de *hacking*.

Configuración de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Después de familiarizarse con los conceptos en URL Filtering Basics (Fundamentos de URL Filtering), estará listo para comenzar con el filtrado de URL. Desde la activación de un licencia de Advanced URL Filtering (si corresponde) hasta probar su configuración, este capítulo cubre lo que necesita para una implementación efectiva del filtrado de URL. Para aprovechar al máximo su implementación, siga las prácticas recomendadas del filtrado de URL.

- Activar licencia de Advanced URL Filtering
- Aspectos básicos de URL Filtering
- Configuración de URL Filtering
- Configurar la categorización en línea
- Excepciones de la categoría de URL
- Prácticas recomendadas de filtrado de URL
- Prueba de la configuración de filtrado de URL

Activar licencia de Advanced URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

La suscripción de Advanced URL Filtering proporciona análisis de URL en tiempo real y prevención de malware. Además del acceso a PAN-DB, la base de datos de filtrado de URL desarrollada por Palo Alto Networks para búsquedas de URL de alto rendimiento, también ofrece cobertura contra URL y direcciones IP maliciosas.

Advanced URL Filtering Las funciones están disponibles en cortafuegos de nueva generación (virtuales y locales), Strata Cloud Manager, Prisma Access (Managed by Panorama), Cloud NGFW para AWS y Cloud NGFW para Azure. Sin embargo, los cortafuegos de nueva generación y Cloud NGFW para Azure requieren una suscripción a Advanced URL Filtering, mientras que todas las licencias de Prisma Access y Cloud NGFW para AWS incluyen capacidades de Advanced URL Filtering.

Para comprobar la compatibilidad de las características de Advanced URL Filtering con cada plataforma de Palo Alto Networks compatible con el filtrado de URL; consulte Compatibilidad con filtrado de URL.

- Strata Cloud Manager
- PAN-OS y Panorama

Activar la licencia de Advanced URL Filtering (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

Vaya a la pestaña **PAN-OS y Panorama** y siga las instrucciones allí para la activación de la licencia.

Si esta usando Strata Cloud Manager:

❑ Valide su licencia de filtrado de URL.

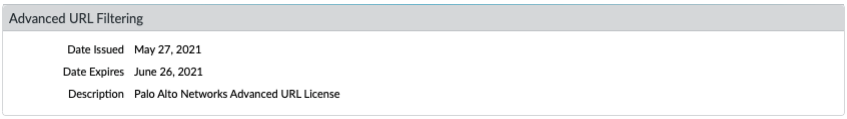
❑ Aspectos básicos de Advanced URL Filtering

Activar licencia de Advanced URL Filtering (PAN-OS y Panorama)

STEP 1 | Obtener e instalar una licencia de Advanced URL Filtering.

La licencia de Advanced URL Filtering incluye acceso a PAN-DB; si la licencia caduca, el cortafuegos deja de realizar todas las funciones de filtrado de URL, la aplicación de categorías de URL y las búsquedas en la nube de URL. Además, todas las otras actualizaciones basadas en la nube no funcionarán hasta que instale una licencia válida.

1. Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y, en la sección Gestión de licencias, seleccione el método de instalación de la licencia:
   - **Retrieve license keys from license server (Recuperar claves de licencia del servidor de licencias)**
   - **Activate feature using authorization code (Activar característica mediante código de autorización)**
2. Confirme que la sección de Advanced URL Filtering, campo **Date Expires (Fecha de caducidad)**, muestra una fecha válida.



Cuando activa la licencia de Advanced URL Filtering, es posible que sus derechos de licencia para PAN-DB y Advanced URL Filtering no se muestren correctamente en el cortafuegos; esta es una anomalía de visualización, no un problema de la licencia, y no afecta el acceso a los servicios. Puede actualizar las licencias en el cortafuegos para rectificar el problema de visualización mediante el siguiente comando de la CLI: ***`request license fetch`***.

STEP 2 | Descargue e instale la última versión de contenido de PAN-OS. El contenido de aplicaciones y amenazas de PAN-OS, versión 8390-6607 y posteriores, permite que los cortafuegos que operan con PAN-OS 9.x y versiones posteriores identifiquen las URL que se han categorizado usando la nueva categoría de detección en tiempo real con Advanced URL Filtering. Para obtener más información sobre la actualización, consulte las notas de la versión del contenido de amenazas y aplicaciones. También puede revisar las Notas de la versión de contenido para aplicaciones y prevención de amenazas en el portal de asistencia técnica de Palo Alto Networks o directamente en la interfaz web del cortafuegos: seleccione **Device (Dispositivo)** > **Dynamic Updates (Actualizaciones dinámicas)** y abra la Release Note (Nota de la versión) de una versión de contenido específica.

Siga las Prácticas recomendadas para las actualizaciones de contenido de aplicaciones y prevención de amenazas *cuando realice una actualización a la versión de contenido más reciente.*

STEP 3 | Programe el cortafuegos para descargar actualizaciones dinámicas para Aplicaciones y amenazas.

Se requiere una licencia de prevención de amenazas para recibir actualizaciones de contenido, la cual cubre Antivirus y Aplicaciones y amenazas.

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. En el campo Schedule de la sección Aplicaciones y amenazas, haga clic en el enlace **None** para programar actualizaciones periódicas.

   Solo puede programar actualizaciones dinámicas si el cortafuegos tiene acceso directo a Internet. Si las actualizaciones ya están programadas en una sección, el texto del enlace muestra la configuración de la programación.

   Las actualizaciones de aplicaciones y amenazas pueden incluir actualizaciones para el filtrado de URL relacionado con Aplicación de búsquedas seguras.

Siguientes pasos:

1. Configure un perfil de filtrado de URL para definir las políticas de uso web de su organización.
2. Pruebe su configuración de filtrado de URL

Aspectos básicos de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

El primer paso para comenzar con el filtrado de URL es comprender los patrones de actividad web de los usuarios en su red.

Para observar estos patrones de forma segura, recomendamos lo siguiente:

- ❑ Revise las Categorías de URL predefinidas de Palo Alto Networks
- ❑ Introduzca las URL en nuestro motor Test A Site para ver cómo PAN-DB las categoriza.
- ❑ Cree un perfil de filtrado de URL (en su mayoría) pasivo que alerte sobre la mayoría de las categorías. Al seleccionar el ajuste `alerta` para una categoría de URL, el cortafuegos registra el tráfico a esa categoría. A continuación, puede ver los sitios a los que acceden los usuarios y decidir el acceso adecuado para las categorías de URL y los sitios específicos.

  *Las alertas sobre toda la actividad web pueden crear un gran número de archivos de logs. Como tal, es posible que solo desee hacer esto como parte de una implementación inicial. En ese momento, también puede reducir los logs de filtrado de URL habilitando la función **Log Container Page Only (Solo página de contenedor de logs)** en el perfil de filtrado de URL para que solo se registre la página principal que coincida con la categoría, no las páginas o categorías posteriores que se puedan cargar dentro de la página contenedora.*
- ❑ Bloquea las categorías de URL que sabemos que son malas: malware, mando y control y phishing.

- Strata Cloud Manager
- PAN-OS y Panorama

Introducción a Advanced URL Filtering (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Utilice Test A Site para comprobar cómo PAN-DB clasifica un sitio web específico.

También puede utilizar la plataforma para solicitar un cambio de categorización de cualquier sitio web que crea que se ha clasificado incorrectamente.

STEP 2 | Cree un perfil de Gestión de acceso URL pasivo que *alerta* en todas las categorías.

El cortafuegos genera una entrada de log del filtrado de URL para sitios web en categorías de URL con una acción distinta de *permitir*.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En Perfiles de gestión de acceso URL, seleccione la casilla situada junto al perfil de prácticas recomendadas y, a continuación, seleccione **Clone (Duplicar)** el perfil.

   El perfil duplicado aparece debajo de los perfiles con el nombre `best-practices-1`.
3. Seleccione el perfil **best-practices-1** y cámbiele el nombre. Por ejemplo, cámbiele el nombre por `url-monitoring`.

STEP 3 | **Alert (Alertar)** en todas las categorías, excepto en malware, comando y control y phishing, que deben permanecer bloqueadas.

1. Debajo **Control de acceso**, seleccione todas las categorías y, a continuación, excluya `malware`, `de comando y controly` `phishing`.
2. Con las categorías aún resaltadas, haga clic en **Set Access (Establecer acceso)** y seleccione **Alert (Alerta)**.
3. **Block (Bloquear)** el acceso a `malware`, `mando y control` y `phishing` otras categorías de URL peligrosas conocidas:
   - phishing
   - dns dinámico
   - unknown
   - extremismo
   - violación de copyright
   - evasión de proxy y anonimizadores
   - dominio recién registrado
   - grayware
   - estacionado
4. Seleccione **Save (Guardar)** el perfil.

STEP 4 | Aplique el perfil de gestión de acceso URL a las reglas de la política de seguridad que permiten el tráfico de los clientes de la zona de confianza a Internet.

Un perfil de gestión de acceso a URL solo está activo cuando se incluye en un grupo de perfiles al que hace referencia una regla de la política de seguridad.

Siga los pasos para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad).

Asegúrese de que la `Zona de origen` en las reglas de la política de seguridad que se aplican a los perfiles de gestión de acceso a URL se establece en una red interna protegida.

STEP 5 | **Push Config (Enviar configuración)** para confirmar la configuración.

STEP 6 | Compruebe los registros de URL para ver a qué categorías del sitio web acceden sus usuarios. Los sitios web bloqueados también se registran.

Para obtener información sobre cómo visualizar los logs y generar informes, consulte la Supervisión de la actividad web.

Seleccione **Activity (Actividad)** > **Log Viewer (Visor de log)** > **URL**. Los informes de filtrado de URL proporcionan una vista de la actividad web en un periodo de 24 horas.

STEP 7 | Siguientes pasos:

- Por todo lo que no permite o bloquea, utilice categorías de riesgo para escribir una política simple basada en la seguridad del sitio web. PAN-DB categoriza cada URL con un nivel de riesgo (alto, medio y bajo). Aunque no se haya confirmado que los sitios de riesgo alto y medio sean sitios malintencionados, guardan una estrecha relación con sitios que sí lo son. Por ejemplo, están en el mismo dominio que sitios malintencionados o han alojado contenido malintencionado hasta hace poco.

  Puede tomar medidas de precaución para limitar especialmente la interacción de sus usuarios con sitios de alto riesgo, ya que puede haber algunos casos en los que desee dar acceso a sus usuarios a sitios que también puedan presentar problemas de seguridad (por ejemplo, es posible que quiera permitir que sus desarrolladores puedan usar blogs de desarrolladores para la investigación, sin embargo, los blogs son una categoría que suele albergar malware).
- Empareje el filtrado de URL con User-ID para controlar el acceso web basado en la organización o departamento, y para bloquear el envío de credenciales corporativas a sitios no autorizados:
  - El filtrado de URL previene el robo de credenciales mediante la detección de envíos de credenciales corporativas a sitios basados en la categoría de sitio. Bloquee a los usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre la introducción de credenciales corporativas en sitios desconocidos o advierta contra la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos.
  - Añada o actualice una regla de la política de seguridad con el perfil de gestión de acceso URL pasivo para que se aplique a un grupo de usuarios de departamento, por ejemplo, marketing o ingeniería. Supervise la actividad del departamento y obtenga comentarios de los miembros del departamento para comprender los recursos web que son esenciales para el trabajo que realizan.
- Considere todas las formas de aprovechar el filtrado de URL para reducir su superficie de ataque. Por ejemplo, una escuela puede usar el filtrado de URL para aplicar la búsqueda segura y estricta para los estudiantes. O bien, si tiene un centro de operaciones de seguridad, puede otorgar acceso con contraseña a sitios comprometidos o peligrosos únicamente a los analistas de amenazas para su investigación.
- Siga las prácticas recomendadas de filtrado de URL.

Empezar con Advanced URL Filtering (PAN-OS & Panorama)

STEP 1 | Utilice Test A Site para comprobar cómo PAN-DB clasifica un sitio web específico.

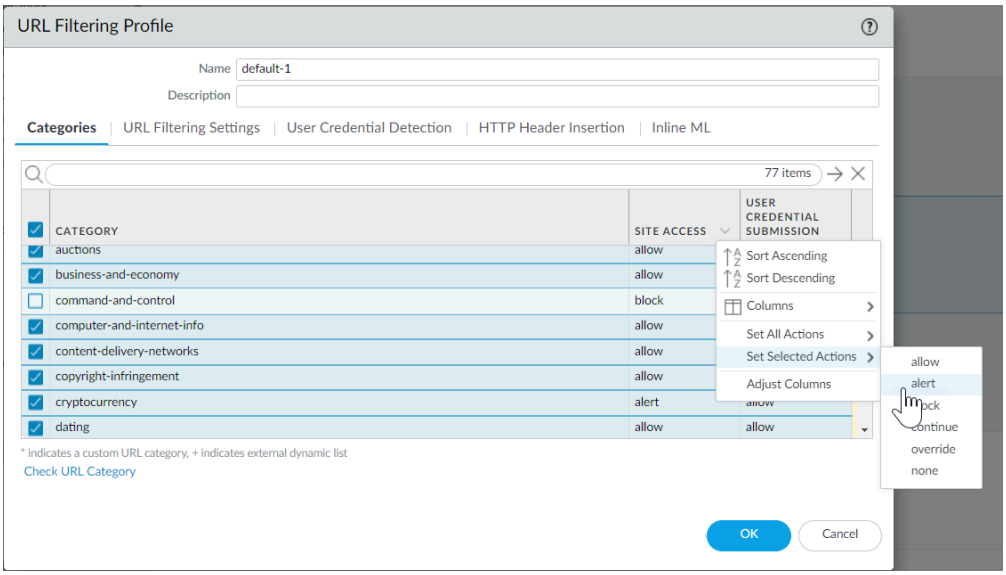
También puede utilizar la plataforma para solicitar un cambio de categorización de cualquier sitio web que crea que se ha clasificado incorrectamente.

STEP 2 | Cree un perfil de filtrado de URL pasivo que *alerte* sobre todas las categorías.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > > **URL Filtering (Filtrado de URL)**.
2. Seleccione el perfil predeterminado y, a continuación, haga clic en **Clone (Duplicar)**. El nuevo perfil se denominará **predeterminado-1**.
3. Seleccione el perfil **predeterminado-1** y cámbiele el nombre. Por ejemplo, cámbiele el nombre por Supervisión-URL.

STEP 3 | Configure en **alert (alertar)** la acción de todas las categorías excepto las de malware, phishing y comando y control, que deben permanecer bloqueadas.

1. En la sección que muestra todas las categorías de URL, seleccione todas las categorías y, a continuación, anule la selección de malware, comando y control y phishing.
2. A la derecha del encabezado de la columna *Acción*, pase el ratón por encima, seleccione la flecha hacia abajo, a continuación, seleccione **Establecer acciones seleccionadas** y seleccione **Alertar**.



3. **Bloquee** el acceso a categorías de URL peligrosas conocidas.

   Bloquee el acceso a las categorías de URL: malware, phishing, DNS dinámico, desconocidas, de comando y control, extremistas, de infracción de derechos de autor, de anonimización y anulación de proxy, de dominio recién registrado, grayware y estacionadas.

4. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 4 | Aplique el perfil de URL Filtering a las reglas de la política de seguridad que permiten el tráfico de clientes en la zona de confianza a Internet.

> *Asegúrese de que la `Zona de origen` en las reglas de la política de seguridad a las que añada perfiles de gestión de acceso URL esté configurada en una red interna protegida.*

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**. Luego, seleccione una regla de la política de seguridad para modificar.
2. En la pestaña **Actions (Acciones)** , edite el ajuste del perfil.
3. Para **Profile Type (Tipo de perfil)**, seleccione **Profiles (Perfiles)**. Aparece una lista de perfiles.
4. Para el perfil de **URL Filtering (Filtrado de URL)**, seleccione el perfil que acaba de crear.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 6 | Visualice los logs de filtrado de URL para consultar todas las categorías de sitios web a las que están accediendo sus usuarios. También se crean logs de las categorías bloqueadas.

Para obtener información sobre cómo visualizar los logs y generar informes, consulte la Supervisión de la actividad web.

Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **URL Filtering (Filtrado de URL)**. Se crea una entrada de log para cualquier sitio web que exista en una categoría de la base de datos de filtrado de URL configurada con una acción distinta de **allow (permitir)**. Los informes de filtrado de URL le ofrecen una vista de la actividad web en un periodo de 24 horas. [**Monitor (Supervisar)** > **Reports (Informes)**].

STEP 7 | Siguientes pasos:

- PAN-DB clasifica cada URL con hasta cuatro categorías, y cada URL tiene una categoría de riesgo (alta, media y baja). Aunque no se haya confirmado que los sitios de riesgo alto y medio sean sitios malintencionados, guardan una estrecha relación con sitios que sí lo son. Por ejemplo, están en el mismo dominio que sitios malintencionados o han alojado contenido malintencionado hasta hace poco. Para todo lo que no permita o bloquee, puede usar categorías de riesgo para escribir reglas de políticas simples basadas en la seguridad del sitio web.

  Puede tomar medidas de precaución para limitar especialmente la interacción de sus usuarios con sitios de alto riesgo, ya que puede haber algunos casos en los que desee dar acceso a sus usuarios a sitios que también puedan presentar problemas de seguridad (por ejemplo, es posible que quiera permitir que sus desarrolladores puedan usar blogs de desarrolladores para la investigación, sin embargo, los blogs son una categoría que suele albergar malware).
- Empareje el filtrado de URL con User-ID para controlar el acceso web basado en la organización o departamento, y para bloquear el envío de credenciales corporativas a sitios no autorizados:
  - El filtrado de URL previene el robo de credenciales mediante la detección de envíos de credenciales corporativas a sitios basados en la categoría de sitio. Bloquee a los

usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre la introducción de credenciales corporativas en sitios desconocidos o advierta contra la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos.

- Añada o actualice una regla de la política de seguridad con el perfil de URL Filtering pasivo para que se aplique a un grupo de usuarios del departamento, por ejemplo, Marketing o Ingeniería [**Policies (Políticas)** > **Security (Seguridad)** > **User (Usuario)**]. Supervise la actividad del departamento y obtenga comentarios de los miembros del departamento para comprender los recursos web que son esenciales para el trabajo que realizan.

- Considere todas las formas de aprovechar el filtrado de URL para reducir su superficie de ataque. Por ejemplo, una escuela puede usar el filtrado de URL para aplicar la búsqueda segura y estricta para los estudiantes. O bien, si tiene un centro de operaciones de seguridad, puede otorgar acceso con contraseña a sitios comprometidos o peligrosos únicamente a los analistas de amenazas para su investigación.
- Siga las prácticas recomendadas de filtrado de URL.

Configuración de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Después de planificar la implementación del filtrado de URL, debe tener una comprensión básica de los tipos de sitios web a los que acceden sus usuarios. Utilice esta información para crear un perfil de URL Filtering que defina cómo el cortafuegos gestiona el tráfico hacia categorías de URL específicas. También puede restringir los sitios a los que los usuarios pueden enviar credenciales corporativas o aplicar una búsqueda segura estricta. Para activar estas configuraciones, aplique el perfil de URL Filtering a las reglas de la política de seguridad que permiten el acceso web.

- Strata Cloud Manager
- PAN-OS y Panorama

Configuración de URL Filtering (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

El filtrado de URL se llama *URL Access Management (Gestión de acceso URL)* en Strata Cloud Manager

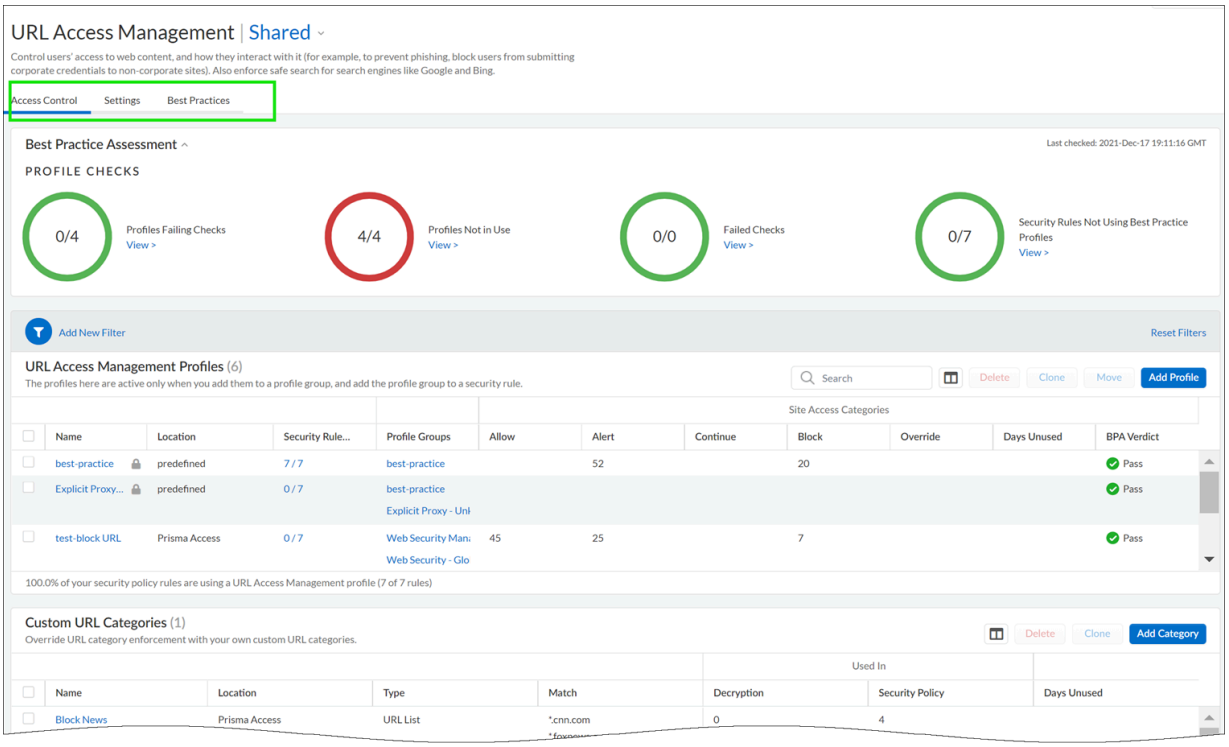
STEP 1 | Compruebe que su suscripción a Prisma Access cubre Advanced URL Filtering.

- Vaya a Gestionar > Configuración del servicio > Descripción general > Licencias para confirmar lo que incluye su suscripción.

STEP 2 | Explorar el panel de gestión de acceso URL.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.

Muévase entre las pestañas **Access Control (Control de acceso)**, **Settings (Configuración)** y **Best Practices (Prácticas recomendadas)** para explorar las funciones de filtrado de URL disponibles.



STEP 3 | Revise y personalice la configuración general de filtrado de URL.

En el panel de control, vaya a **Settings (Configuración)** para ver la configuración predeterminada de filtrado de URL que se aplica en todo el entorno de Prisma Access, incluido:

- Ajustes de tiempo de espera y búsqueda de filtrado de URL
- Anulaciones de filtrado de URL para ciertos administradores
- Páginas de respuesta de filtrado de URL
- Configuración de Aislamiento remoto del navegador (RBI)

Anexa automáticamente tokens finales a las URL de una categoría de URL personalizada o lista dinámica externa

(PAN-OS 10.1 y anteriores) Si añade las URL a las categorías de URL personalizadas o listas dinámicas externas (EDL) de tipo lista de URL y no añade una barra inclinada (/), puede bloquear o permitir más URL de las previstas. Por ejemplo, introducir ***`example.com`*** *en lugar de* ***`example.com/`*** *expande las URL coincidentes a example.com.website.info o example.com.br. Prisma Access puede añadir automáticamente una barra inclinada a las URL en categorías de URL personalizadas o EDL para que, si introduce* ***`example.com`****, Prisma Access lo trate como trataría* ***`ejemplo.com/`*** *y solo considere que ese dominio y sus subdirectorios coinciden. Vaya a* ***Settings (Configuración)*** *>* ***General Settings (Configuración general)*** *y habilite la opción* ***Append End Token to Entries (Anexar el token final a las entradas)****.*

(PAN-OS 10.2 y posterior)Prisma Access añade automáticamente una barra inclinada a las entradas de dominio.

Puede personalizar esta configuración para cada tipo de implementación (usuarios móviles, redes remotas o conexiones de servicio).

STEP 4 | Crear un perfil de Gestión de acceso URL.

En el panel de gestión de acceso URL, debe **Add Profile (Añadir perfil)** y especificar la configuración de acceso web:

- **Access Control (Control de acceso)** muestra las categorías URL y listas para las que puede definir el acceso web y la política de uso. De forma predeterminada, los permisos del **Site**

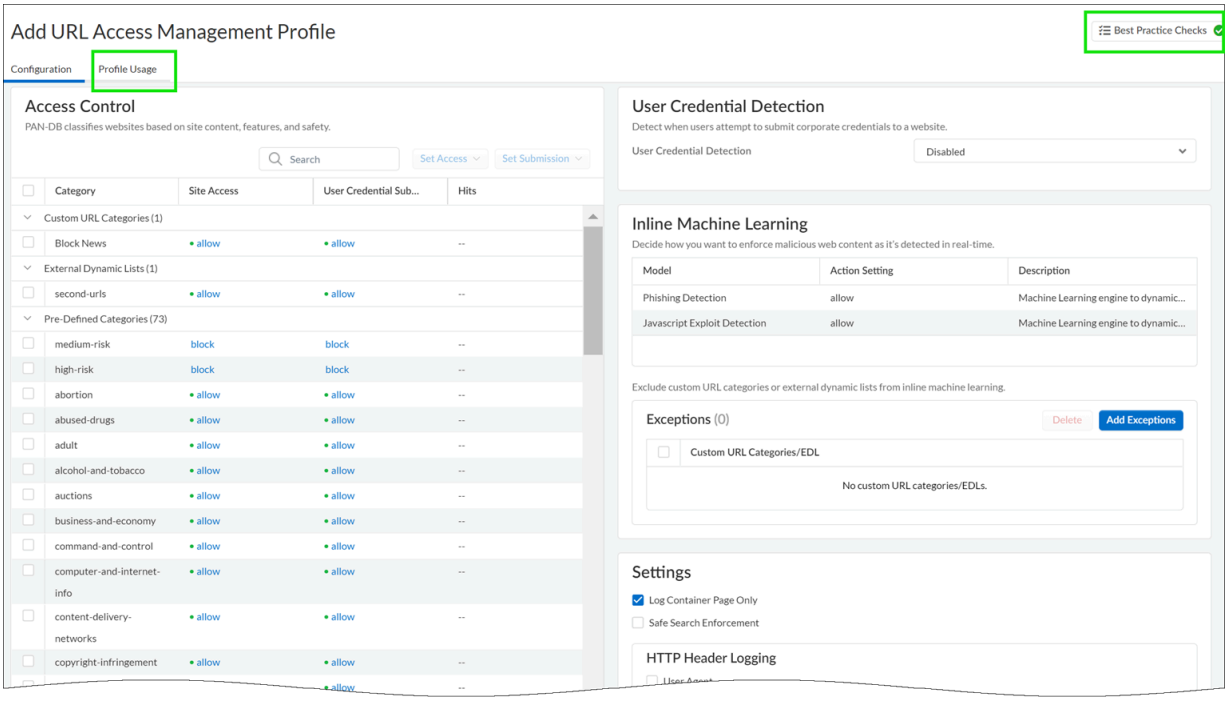
Access (Acceso al sitio) y el **User Credential Submission (Envío de credencial de usuario)** para todas las categorías se establecen en **Allow (Permitir)**.

- Para cada categoría de URL, configure **User Credential Detection (Detección de credenciales de usuario)** para que los usuarios puedan enviar credenciales solo a sitios en categorías de URL especificadas.
- Habilite la **Safe Search Enforcement (Aplicación de búsquedas seguras)** para hacer cumplir el estricto filtrado de búsquedas seguras.
- Habilite **Log Container Page Only (Solo página de contenedor de logs)** para registrar solo las URL que coincidan con el tipo de contenido especificado.
- La activación de **HTTP Header Logging (Registro de logs del encabezado HTTP)** proporciona visibilidad sobre los atributos incluidos en la solicitud de HTTP enviada a un servidor.
- Utilice la **Advanced URL Inline Categorization (Categorización avanzada de URL en línea)** para habilitar y configurar el análisis de páginas web en tiempo real y gestionar excepciones de URL.
  - **Enable local Inline Categorization (Habilitar categorización en línea local)**: permite el análisis en tiempo real del tráfico de URL mediante modelos de aprendizaje automático para detectar y evitar que las variantes maliciosas de phishing y las vulnerabilidades de JavaScript entren a su red.
  - **Enable cloud Inline Categorization (Habilitar categorización en línea en la nube)**: permite el análisis en tiempo real de URL mediante el reenvío del contenido de páginas web sospechosas a la nube para un análisis complementario. Utiliza detectores basados en aprendizaje automático que complementan los motores de análisis utilizados por el aprendizaje automático local en línea.

- Puede definir **Exceptions (Excepciones)** de URL para sitios web específicos para excluir de las acciones de aprendizaje automático en línea.

Tenga en cuenta que:

- Las comprobaciones de prácticas recomendadas están integradas en el perfil para brindarle una evaluación en tiempo real de su configuración.
- Una vez que haya terminado de habilitar un perfil, puede examinar el uso del perfil para ver si alguna regla de la política de seguridad hace referencia al perfil.



STEP 5 | Aplique el perfil de Gestión de acceso URL a una regla de la política de seguridad.

Un perfil de gestión de acceso URL solo está activo cuando se incluye en un grupo de perfiles al que hace referencia una regla de la política de seguridad.

Siga los pasos para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad). Asegúrese de **Push Config (Enviar configuración)**

Configuración de URL Filtering (PAN-OS y Panorama)

STEP 1 | Cree un perfil de filtrado de URL.

Si aún no lo tiene, configure un perfil de filtrado de URL recomendado para garantizar protección contra las URL que alojan malware o contenido de exploits.

Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de URL.

STEP 2 | Defina el acceso al sitio para cada categoría de URL.

Seleccione **Categories (Categorías)** y configure el acceso al sitio para cada categoría de URL:

- **Permita** el tráfico destinado a esa categoría de URL; el tráfico permitido no está registrado.
- Seleccione **alert (alerta)** para tener visibilidad sobre los sitios a los que los usuarios están accediendo. La coincidencia de tráfico para la categoría está permitida, pero un log de filtrado de URL se genera para registrar cuando un usuario accede a un sitio de la categoría.
- Seleccione **block (bloquear)** para denegar el acceso al tráfico que coincide con la categoría y registrar en logs el tráfico bloqueado.
- Seleccione **continue (continuar)** para mostrar una página a los usuarios con una advertencia y solicitarles que hagan clic en **Continue (Continuar)** para proceder a un sitio de la categoría.
- Para permitir el acceso solo si los usuarios especifican una contraseña configurada, seleccione **override (anular)**. Para obtener más información, consulte Habilitación del acceso a determinados sitios mediante contraseña.

STEP 3 | Configure el perfil de filtrado de URL para detectar envíos de credenciales corporativas a sitios web que están en categorías URL permitidas.

El cortafuegos omite automáticamente la comprobación de los envíos de credenciales para App-ID™ asociados con los sitios que nunca se ha observado que alojan malware o contenido de phishing (suplantación de identidad), para garantizar un desempeño óptimo y una tasa de falsos positivos baja, incluso si habilita las comprobaciones en la categoría correspondiente. La lista de sitios en los cuales el cortafuegos omitirá la comprobación de credenciales se actualiza automáticamente a través de las actualizaciones de aplicación y contenido de prevención de amenazas.

1. Seleccione **User Credential Detection (Detección de credencial de usuario)**.
2. Seleccione uno de los métodos para comprobar los envíos de credenciales corporativas a páginas web en la lista desplegable **User Credential Detection (Detección de credenciales de usuario)**:
   - **Use IP User Mapping (Usar asignación de usuarios IP):** comprueba el envío de nombres de usuario corporativo válidos y verifica que el nombre de usuario coincida con el usuario registrado en la dirección IP de origen de la sesión. El cortafuegos compara el nombre de usuario enviado con su tabla de asignación de direcciones IP a nombres de usuario. Puede emplear cualquiera de los métodos de asignación de usuarios descritos en Asignación de direcciones IP a los usuarios.

- **Use Domain Credential Filter (Usar filtro de credenciales de dominio)**: comprueba el envío de nombres de usuario y contraseñas válidas, y verifica que el nombre de usuario esté asignado a la dirección IP del usuario registrado. Consulte Configuración de detección de credenciales con el agente de User-ID de Windows para obtener instrucciones sobre cómo configurar User-ID para habilitar este método.
- **Use Group Mapping (Usar asignación de grupo)**: comprueba el envío de nombres de usuario válidos en función de la tabla de asignación de usuario a grupo completada cuando configura el cortafuegos para la asignación de usuarios a grupos.

  Con la asignación de grupos, usted puede aplicar la detección de credenciales a **cualquier** parte del directorio o a un grupo específico, tal como grupos como TI que tienen acceso a sus aplicaciones más sensibles.

Este método es propenso a falsos positivos en entornos que no tienen nombres de usuario estructurados de manera única, por lo que solo debe usar este método para proteger sus cuentas de usuario valiosas.

3. Configure la **Valid Username Detected Log Severity (Gravedad del log detectado de nombre de usuario válido)** que el cortafuegos utilizará para la detección de logs de envío de credenciales corporativas (el valor predeterminado es media).

STEP 4 | Configure el perfil de filtrado de URL para detectar phishing y JavaScript malicioso en tiempo real mediante la categorización en línea local.

STEP 5 | Habilite o bloquee a los usuarios para el envío de credenciales corporativas a sitios en función de la categoría de URL para la prevención del phishing de credenciales.

El cortafuegos omite automáticamente la comprobación de los envíos de credenciales para App-ID asociados con los sitios que nunca se ha observado que alojan malware o contenido de phishing (suplantación de identidad), para garantizar un desempeño óptimo y una tasa de falsos positivos baja, incluso si habilita las comprobaciones en la categoría correspondiente. La lista de sitios en los cuales el cortafuegos omitirá la comprobación de credenciales se actualiza automáticamente a través de las actualizaciones de aplicación y contenido de prevención de amenazas.

1. Para cada categoría de URL a la cual se permite el **acceso al sitio**, seleccione cómo desea que se manejen los **envíos de credenciales de usuario**:
   - **alert (alerta)**: permite que los usuarios envíen sus credenciales al sitio web, pero genera un log de alerta de filtrado de URL cada vez que un usuario envía credenciales a sitios de esta categoría de URL.
   - **allow (permitir)**: (predeterminado) permite que los usuarios envíen sus credenciales al sitio web.
   - **block (bloquear)**: muestra la página de bloqueo antiphishing para bloquear a los usuarios para el envío de credenciales al sitio web.
   - **continue (continuar)**: presenta la página de continuación antiphishing, que requiere que los usuarios hagan clic en **Continue (Continuar)** para acceder al sitio.
2. Configure el perfil de filtrado de URL para detectar envíos de credenciales corporativas a sitios web en categorías de URL permitidas.

STEP 6 | Defina excepciones de categoría de URL para especificar sitios web que siempre deben estar bloqueados o estar permitidos, independientemente de la categoría de URL.

Por ejemplo, para reducir los logs de filtrado de URL, es posible que desee añadir sus sitios web corporativos a la lista de permitidos para que no se generen logs para esos sitios o, si hay un sitio web que se usa demasiado y no está relacionado con el trabajo, puede añadirlo a la lista de bloqueo.

Las acciones de política configuradas para categorías de URL personalizadas tienen prioridad sobre las URL coincidentes en listas dinámicas externas.

El tráfico de los sitios web que se encuentran en la lista de bloqueados siempre se bloquea independientemente de la acción de la categoría asociada. El tráfico de las URL que se encuentra en la lista de permitidos siempre está permitido.

Para obtener más información sobre el formato correcto y el uso de comodines, consulte las Directrices para las excepciones de categoría de URL.

STEP 7 | Habilite Aplicación de búsquedas seguras.

STEP 8 | Registre solo la página que visita un usuario para eventos de filtrado de URL.

1. Seleccione **URL Filtering Settings (Configuración de URL Filtering)** y habilite **Log container page only (Solo página de contenedor de logs)** (predeterminado) para que el cortafuegos registre solo la página principal que coincide con la categoría, no las páginas o categorías posteriores que se cargan dentro de la página del contenedor.
2. Para habilitar la creación de logs para todas las páginas y categorías, deshabilite la opción **Log container page only (Registrar solo página de contenedor)**.

STEP 9 | Habilite HTTP Header Logging (Registro de encabezado HHTTP) para uno o varios de los campos de encabezado HTTP admitidos.

Seleccione **URL Filtering Settings (Configuración de filtrado de URL)** y seleccione uno o varios de los siguientes campos para registrar:

- **User-Agent (Agente de usuario)**
- **Referer (Sitio de referencia)**
- **X-Forwarded-For**

STEP 10 | Guardar el perfil de filtrado de URL.

Haga clic en **OK (Aceptar)**.

STEP 11 | Aplique el perfil de URL Filtering a las reglas de la política de seguridad que permiten el tráfico de clientes en la zona de confianza a Internet.

> *Asegúrese de que la `Zona de origen` en las reglas de la política de seguridad a la que añade perfiles de URL Filtering esté configurada en una red interna protegida.*

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**. Luego, seleccione una regla de la política de seguridad para modificar.
2. En la pestaña **Actions (Acciones)** , edite el ajuste del perfil.
3. Para **Profile Type (Tipo de perfil)**, seleccione **Profiles (Perfiles)**. Aparece una lista de perfiles.
4. Para el perfil de **URL Filtering (Filtrado de URL)**, seleccione el perfil que acaba de crear.
5. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 12 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 13 | Pruebe su configuración de filtrado de URL

STEP 14 | (Práctica recomendada) Habilite la opción **Hold client request for category lookup (Retener solicitud de cliente para búsqueda de categoría)** para bloquear las solicitudes de cliente mientras el cortafuegos realiza búsquedas de categorías de URL.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content ID (ID de contenido)**.
2. Seleccione **Hold client request for category lookup (Retener solicitud de cliente para búsqueda de categoría)**.
3. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 15 | Establezca la cantidad de tiempo, en segundos, antes de que se agote el tiempo de espera de una búsqueda de categoría de URL.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **icono de engranaje**.
2. Introduzca un número para **Category lookup timeout (sec) [Tiempo de espera de búsqueda de categoría (seg)]**.
3. Haga clic en **OK (Aceptar)**.
4. Haga clic en **Commit (Confirmar)** para compilar los cambios.

Configurar la categorización en línea

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Para habilitar la categorización en línea, adjunte un perfil de filtrado de URL configurado con la configuración de categorización en línea a una Regla de política de seguridad (consulte Configurar una política de seguridad básica).

La categorización local en línea de filtrado de URL no se admite actualmente en el dispositivo virtual VM-50 o VM50L.

- Strata Cloud Manager
- PAN-OS y Panorama

Configurar la categorización en línea (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

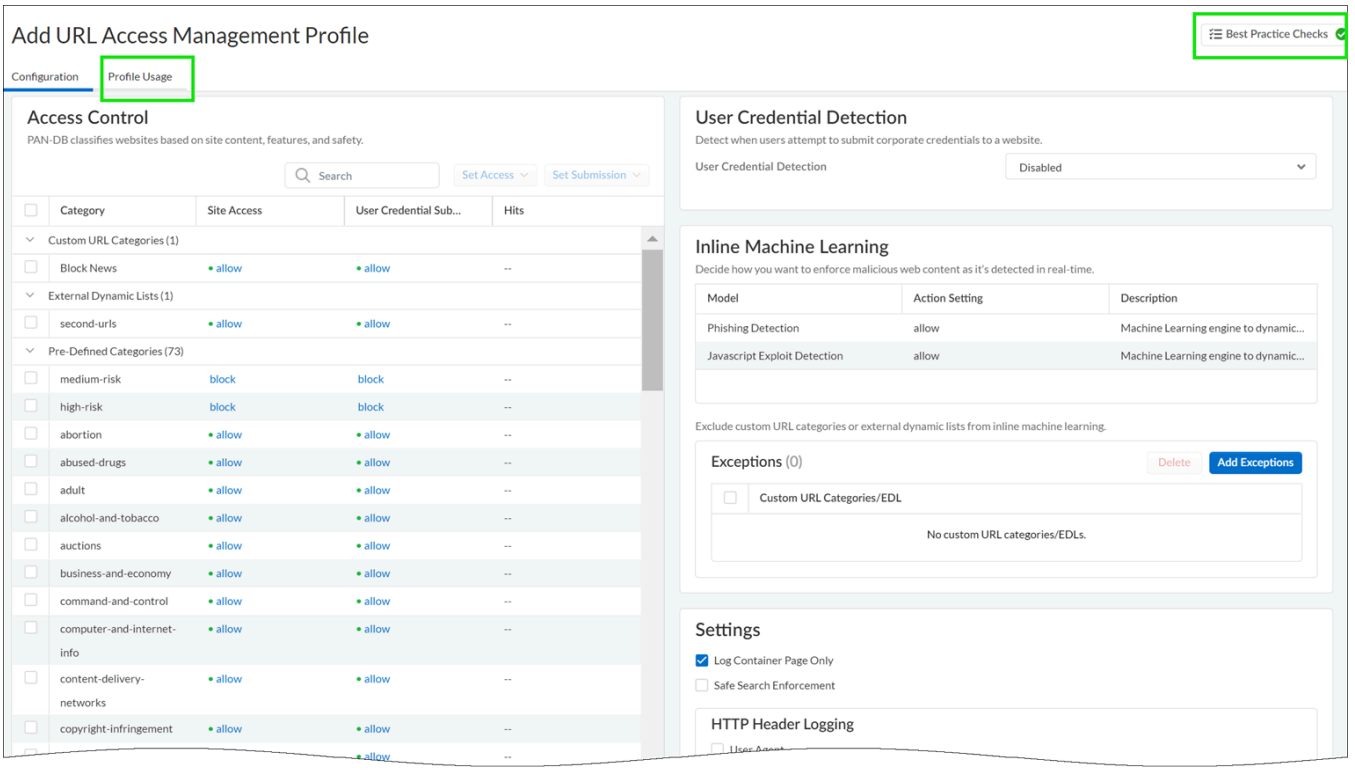
STEP 1 | Actualice o cree un perfil de gestión de acceso URL.

1. Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En el panel de control de gestión de acceso URL, seleccione un perfil de gestión de acceso URL o **Add Profile (Añadir perfil)**.

   Si crea un nuevo perfil, configure los ajustes en el perfil, como el acceso al sitio para las categorías de URL [**Access Control (Control de acceso)**]. Configurar el filtrado de URL (gestión de la nube) describe los ajustes disponibles.
3. En **Advanced URL Inline Categorization (Categorización avanzada de URL en línea)**, seleccione un tipo de categorización en línea.

   Ambas opciones permiten el análisis de páginas web en tiempo real y gestionan las excepciones de URL.

- **Enable cloud Inline Categorization (Habilitar categorización en línea en la nube)**: permite el análisis en tiempo real de URL mediante el reenvío del contenido de páginas web sospechosas a la nube para un análisis complementario. Utiliza detectores basados en aprendizaje automático que complementan los motores de análisis utilizados por el aprendizaje automático local en línea.
- **Enable local Inline Categorization (Habilitar categorización en línea local)**: permite el análisis en tiempo real del tráfico de URL mediante modelos de aprendizaje automático para detectar y evitar que las variantes maliciosas de phishing y las vulnerabilidades de JavaScript entren a su red.
- También puede definir la **Exceptions (Excepciones)** de URL para excluir sitios web específicos de las acciones de aprendizaje automático en línea.



4. Seleccione **Save (Guardar)** el perfil.

STEP 2 | Aplique el perfil de Gestión de acceso URL a una regla de la política de seguridad.

Para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad), añádalo al `grupo de perfiles` y haga referencia al grupo de perfiles en una regla de la política de seguridad.

Configurar la categorización en línea (PAN-OS y Panorama)

En PAN-OS 10.2, la función URL Filtering Inline ML, o aprendizaje automático en línea de URL Filtering, se ha cambiado a Categorización en línea. Como resultado, la tarea PAN-OS 10.1 utiliza la frase Aprendizaje automático en línea de filtrado de URL, mientras que la tarea PAN-OS 10.2 y posterior utiliza Categorización en línea. Para obtener más información, revise la entrada Aprendizaje automático en línea de URL Filtering en Consideraciones sobre el cambio a versiones anteriores/posteriores de PAN-OS 10.2.

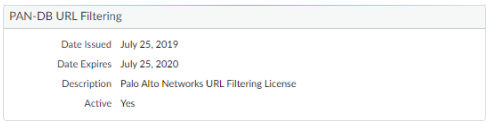
- PAN-OS 10.1
- PAN-OS 10.2 y posterior

Configurar la categorización en línea (PAN-OS 10.1)

STEP 1 | Inicie sesión en la interfaz web de PAN-OS.

STEP 2 | Compruebe que tiene una suscripción activa de URL Filtering heredado o de Advanced URL Filtering.

Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y confirme que la licencia de filtrado de URL está disponible y no ha caducado.

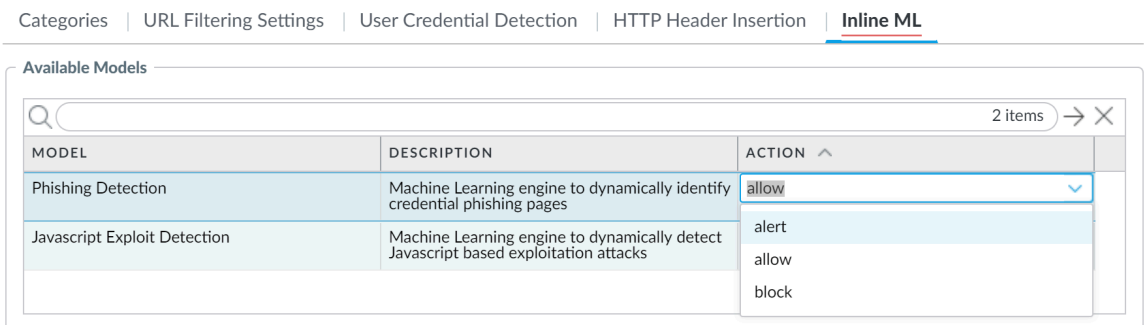


STEP 3 | Configure los ajustes del aprendizaje automático en línea de URL Filtering en un perfil de filtrado de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y, a continuación, **añada** o seleccione un perfil de filtrado de URL.
2. Seleccione **Inline ML (Aprendizaje automático en línea)** y defina una **Action (Acción)** para cada modelo de aprendizaje automático en línea.

   Hay dos motores de clasificación disponibles para cada tipo de contenido malicioso de la página web: **Phishing** y **JavaScript Exploit (Exploit de JavaScript)**.

   - **Block (Bloquear)**: cuando el cortafuegos detecta un sitio web con contenido de phishing, genera una entrada de log de filtrado de URL.
   - **Alerta**: el cortafuegos permite el acceso al sitio web y genera una entrada de log de filtrado de URL.
   - **Permitir**: el cortafuegos que permite el acceso al sitio web pero no genera una entrada de log de filtrado de URL.



3. Haga clic en **OK (Aceptar)** para guardar los cambios.
4. Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 4 | (Opcional) Añada excepciones de URL a su perfil de filtrado de URL si encuentra falsos positivos.

Puede añadir excepciones especificando una lista dinámica externa en el perfil de filtrado de URL o añadiendo una entrada de página web desde los logs de filtrado de URL a una categoría URL personalizada.

1. Seleccione **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > URL Filtering (Filtrado de URL)**.
2. Seleccione el perfil de filtrado de URL para el que desee excluir URL específicas y, a continuación, seleccione **Inline ML (Aprendizaje automático en línea)**.
3. Debe **Add (Añadir)** una lista dinámica externa preexistente del tipo de URL. Si no hay ninguno disponible, cree una nueva lista dinámica externa.
4. Haga clic en **OK (Aceptar)** para guardar los cambios.
5. Haga clic en **Commit (Confirmar)** para compilar los cambios.

Añada excepciones de archivos a partir de las entradas de log de filtrado de URL.

1. Seleccione **Monitor (Supervisar) > Logs > URL Filtering (Filtrado de URL)** y filtre los logs para las entradas de URL con un veredicto de aprendizaje automático en línea de **malicious-javascript (javascript malicioso)** o **phishing**. Seleccione un log de filtrado de URL para una URL para la que desea crear una excepción.
2. Vaya a la **vista de log detallada** y desplácese hacia abajo hasta el panel **Details (Detalles)** y, a continuación, seleccione **Create Exception (Crear excepción)** que se encuentra junto al **Inline ML Verdict (Veredicto de aprendizaje automático en línea)**.

3. Seleccione una categoría personalizada para la excepción de URL y haga clic en **OK (Aceptar)**.

   La nueva excepción de URL se puede encontrar en la lista a la que se añadió en **Objects (Objetos) > Custom Objects (Objetos personalizados) > URL Category (Categoría de URL)**.

STEP 5 | (Opcional) Verifique el estado de la conectividad del cortafuegos con el servicio en la nube de aprendizaje automático en línea.

Utilice el siguiente comando de la CLI en el cortafuegos para ver el estado de la conexión.

```
show mlav cloud-status
```

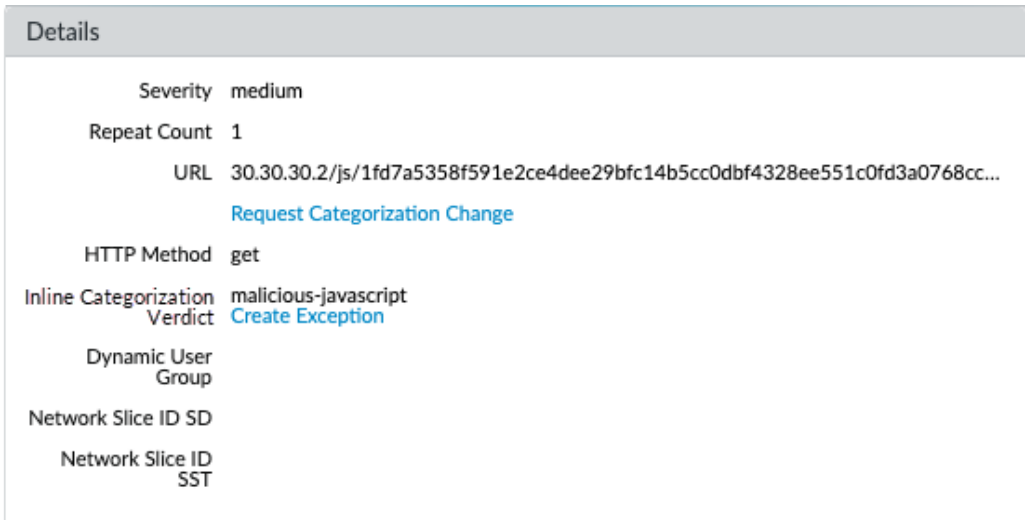
Por ejemplo:

```
show mlav cloud-status MLAV cloud Current cloud server:
 ml.service.paloaltonetworks.com Cloud connection: connected
```

Si no puede conectarse al servicio en la nube de ML en línea, compruebe que el dominio ML ml.service.paloaltonetworks.com no esté bloqueado.

STEP 6 | Probar la implementación de filtrado de URL

Para ver información sobre las páginas web que se han procesado mediante el aprendizaje automático en línea de URL Filtering, filtre los logs [**Monitor (Supervisar) > Logs > URL Filtering (Filtrado de URL)**] según el **Inline ML Verdict (Veredicto de aprendizaje automático en línea)**. Las páginas web que se ha determinado que contienen amenazas se clasifican con veredictos de **phishing** o **malicious-javascript (javascript malicioso)**. Por ejemplo:



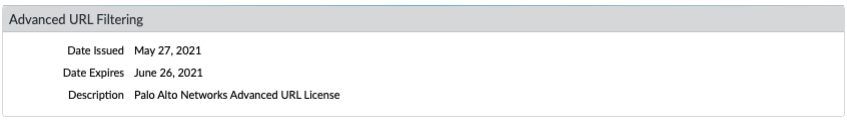
Configurar la categorización en línea (PAN-OS 10.2 y versiones posteriores)

STEP 1 | Inicie sesión en la interfaz web de PAN-OS.

STEP 2 | Para aprovechar la categorización en línea, debe tener una suscripción de Advanced URL Filtering activa.

> *La categorización local en línea se puede habilitar si es titular preexistente de una suscripción de filtrado de URL heredada.*

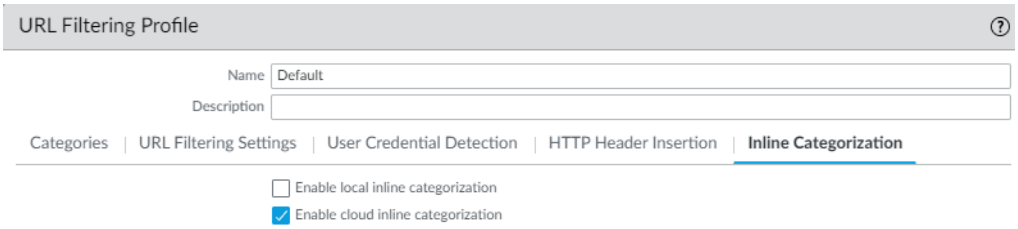
Compruebe que tiene una suscripción de Advanced URL Filtering. Para verificar las suscripciones para las que tiene licencias actualmente activas, seleccione **Device (Dispositivo) > Licenses (Licencias)** y verifique que las licencias correspondientes estén disponibles y no estén vencidas.



STEP 3 | Actualice o cree un nuevo perfil de filtrado de URL para habilitar la categorización en la nube en línea.

*La acción de política utilizada por la categorización local y en la nube en línea depende de la configuración configurada en la pestaña **Categories (Categorías)**.*

1. Seleccione un **perfil de filtrado de URL** existente o **añada** uno nuevo [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**].
2. Seleccione su perfil de filtrado de URL y luego vaya a **Inline Categorization (Categorización en línea)** y habilite los métodos de categorización en línea que desea implementar.
   - **Habilite la categorización en línea en la nube**: un motor de aprendizaje profundo en línea basado en la nube que analiza el contenido sospechoso de la página web en tiempo real para proteger a los usuarios contra ataques web de día cero, incluidos los ataques de phishing dirigidos y otros ataques basados en la web que utilizan técnicas avanzadas de evasión.
   - **Habilite la categorización local en línea**: un motor de detección basado en cortafuegos que utiliza técnicas de aprendizaje automático para evitar variantes maliciosas de explotaciones de JavaScript y ataques de phishing incrustados en páginas web.



3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 4 | (Opcional) Añada excepciones de URL a su perfil de filtrado de URL si encuentra falsos positivos. Puede añadir excepciones especificando una lista dinámica externa o una lista de categorías de URL personalizada en el perfil de URL Filtering. Las excepciones especificadas se aplican tanto a la categorización en línea local como en la nube.

*Las excepciones de URL creadas a través de otros mecanismos que añaden entradas a la categoría de URL personalizada (**Objects [Objetos]** > **Custom Objects [Objetos personalizados]** > **URL Category [Categoría de URL]**)*

también pueden funcionar como excepciones para la categorización en línea.

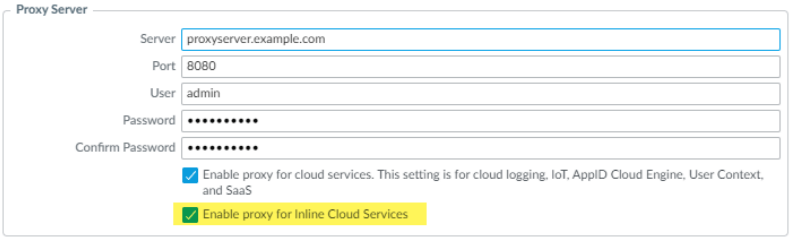
1. Seleccione **Objects (Objetos) > Security Profiles (Perfiles de seguridad) > URL Filtering (Filtrado de URL)**.
2. Seleccione un perfil de filtrado de URL para el que desee excluir direcciones URL específicas y, a continuación, seleccione **Inline Categorization (Categorización en línea)**.
3. Haga clic en **Add (Añadir)** para seleccionar una lista dinámica externa basada en URL preexistente o una categoría de URL personalizada. Si no hay ninguno disponible, cree una nueva lista dinámica externa o una categoría de URL personalizada, respectivamente.
4. Haga clic en **OK (Aceptar)** para guardar el perfil de filtrado de URL y **confirmar** los cambios.

STEP 5 | (Necesario cuando el cortafuegos se implementa con un servidor proxy explícito) Configure el servidor proxy utilizado para acceder a los servidores que facilitan las solicitudes

generadas por todas las características de análisis en la nube configuradas. Se puede especificar un único servidor proxy que se aplica a todos los servicios de actualización de Palo Alto Networks, incluidos todos los servicios de registro de logs y nube en línea configurados.

1. (PAN-OS 11.2.3 y posterior) Configure el servidor proxy a través de PAN-OS.
   1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Services (Servicios)** y edite la sección detalles de **Services (Servicios)**.
   2. Especifique la configuración del **Proxy Server (Servidor proxy)** y **Enable proxy for Inline Cloud Services (Habilitar el proxy para servicios en la nube en línea)**. Puede proporcionar una dirección IP o FQDN en el campo **Server (Servidor)**.

      La contraseña del servidor proxy debe contener un mínimo de seis caracteres.

   3. Haga clic en **OK (Aceptar)**.
2. (Solo para las siguientes versiones: PAN-OS 10.2.11 y versiones posteriores y PAN-OS 11.1.5 y versiones posteriores) Configure el servidor proxy a través de la CLI del cortafuegos.
   1. Acceda a la CLI del cortafuegos.
   2. Configure los ajustes del servidor proxy base mediante los siguientes comandos de la CLI:

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
      ```



```
set deviceconfig system secure-proxy-user <value> set
deviceconfig system secure-proxy-password <value>
```

La contraseña del servidor proxy debe contener un mínimo de seis caracteres.

3. Habilite el servidor proxy para enviar solicitudes a los servidores de servicios en la nube en línea mediante el siguiente comando de la CLI:

```
debug dataplane mica set inline-cloud-proxy enable
```

4. Vea el estado operativo actual del soporte de proxy para los servicios en la nube en línea mediante el siguiente comando de la CLI:

```
debug dataplane mica show inline-cloud-proxy
```

Por ejemplo:

```
debug dataplane mica show inline-cloud-proxy Proxy for
 Advanced Services is Disabled
```

STEP 6 | (Opcional) Establezca el nombre de dominio completo (FQDN) de contenido en la nube que utiliza el cortafuegos para gestionar las solicitudes de servicio de categorización en línea. El FQDN predeterminado se conecta a hawkeye.services-edge.paloaltonetworks.com y, a continuación, se resuelve en el servidor de servicios en la nube más cercano. Puede anular la selección automática del servidor especificando un servidor de contenido en la nube regional que mejor se adapte a sus requisitos de residencia y rendimiento de datos.

El FQDN de contenido en la nube es un recurso utilizado globalmente y afecta a la forma en que otros servicios que dependen de esta conexión envían cargas útiles de tráfico.

Verifique que el cortafuegos use el FQDN de Content Cloud correcto (**Device [Dispositivo]** > **Setup [Configuración]** > **Content-ID** > **Content Cloud Setting [Configuración de Content Cloud]**) para su región y cambie el FQDN si es necesario:

- EE. UU.: **us.hawkeye.services-edge.paloaltonetworks.com**
- Europa: **eu.hawkeye.services-edge.paloaltonetworks.com**
- Reino Unido:**uk.hawkeye.services-edge.paloaltonetworks.com**

  El FQDN de contenido en la nube con sede en el Reino Unido proporciona soporte de servicio de categorización en línea de Advanced URL Filtering al conectarse al servicio de backend ubicado en la UE (eu.hawkeye.services-edge.paloaltonetworks.com).
- APAC: **apac.hawkeye.services-edge.paloaltonetworks.com**

STEP 7 | (Opcional) Verifique el estado de la conectividad del cortafuegos con los servidores de categorización en línea.

1. El servidor ml.service.paloaltonetworks.com proporciona actualizaciones periódicas para los componentes basados en cortafuegos relacionados con el funcionamiento de la nube y la categorización local en línea.

   Utilice el siguiente comando de la CLI en el cortafuegos para ver el estado de la conexión.

   ```
   show mlav cloud-status
   ```

   Por ejemplo:

   ```
   show mlav cloud-status MLAV cloud Current cloud server:
    ml.service.paloaltonetworks.com Cloud connection: connected
   ```

   Si no puede conectarse al servicio en la nube de aprendizaje automático en línea, verifique que el siguiente dominio no esté bloqueado: ml.service.paloaltonetworks.com.

2. El servidor hawkeye.services-edge.paloaltonetworks.com es utilizado por la categorización en la nube en línea para manejar las solicitudes de servicio.

   Utilice el siguiente comando de la CLI en el cortafuegos para ver el estado de la conexión.

   ```
   show ctd-agent status security-client
   ```

   Por ejemplo:

   ```
   show ctd-agent status security-client ... Security Client
    AceMlc2(1) Current cloud server: hawkeye.services-
   edge.paloaltonetworks.com Cloud connection: connected ...
   ```

   Resultado de CLI acortado por brevedad.

   Si no puede conectarse al servicio en la nube de Advanced URL Filtering, compruebe que no se está bloqueando el siguiente dominio: hawkeye.services-edge.paloaltonetworks.com.

STEP 8 | Instale un certificado de dispositivo de cortafuegos actualizado que se use para autenticarse en el servicio en la nube de Advanced URL Filtering. Repita el procedimiento para todos los cortafuegos habilitados para la categorización en la nube en línea.

STEP 9 | Probar la implementación de filtrado de URL

Excepciones de la categoría de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Puede excluir sitios web específicos de la aplicación de la categoría de URL, lo que garantiza que los sitios web se bloqueen o permitan independientemente de la acción de política asociada con sus categorías de URL. Por ejemplo, puede bloquear la categoría de URL de redes sociales pero permitir el acceso a LinkedIn. Para crear excepciones a la aplicación de políticas de categoría de URL:

- Añada las direcciones IP o URL de los sitios que desea bloquear o permitir a una categoría URL personalizada de tipo **URL List (Lista de URL)**. Luego, defina el acceso al sitio para la categoría en un perfil de filtrado de URL. Por último, adjunte el perfil a una regla de la política de seguridad.

  También puede usar una categoría de URL personalizada como criterio de coincidencia en una regla de la política de seguridad. Asegúrese de colocar la regla de excepción sobre cualquier regla que bloquee o permita las categorías a las que pertenecen las excepciones de URL.

- Añada las URL de los sitios que desea bloquear o permitir a una lista dinámica externa de tipo **URL List (Lista de URL)**. Luego, utilice una lista dinámica externa en un perfil de filtrado de URL o como criterio de coincidencia en una regla de política de seguridad. La ventaja de usar una lista dinámica externa es que puede actualizar la lista sin realizar un cambio de configuración o compilación en el cortafuegos.

  *Las listas dinámicas externas de tipo **URL List (Lista de URL)** no deben confundirse con las listas dinámicas externas de tipo Lista de dominio o Lista de direcciones IP. Si bien las listas dinámicas externas de URL permiten dominios y direcciones IP, lo contrario no es cierto y da como resultado entradas no válidas.*

- Directrices para las excepciones de categoría de URL
- Creación de una categoría de URL personalizada
- Usar una lista dinámica externa en un perfil de filtro de URL

Directrices para las excepciones de categoría de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Las siguientes pautas describen cómo llenar listas de excepciones de categorías de URL: categorías de URL personalizadas o listas dinámicas externas de URL. Ofrecemos ejemplos de cómo usar comodines y entradas específicas.

Pautas básicas para las listas de excepción de categoría de URL

Considere las coincidencias potenciales que podría tener una entrada antes de añadirla a una lista de excepción de categoría de URL. Las siguientes pautas especifican cómo crear una entrada que bloquee o permita los sitios web y las páginas que desee.

De forma predeterminada, el cortafuegos agrega automáticamente una barra inclinada final (/) a las entradas de dominio que no terminan en una barra inclinada final (/) o un asterisco (*). La adición de la barra diagonal final cambia las URL que el cortafuegos considera coincidentes y para las que aplica la política. En las entradas de dominio que no son comodines, la barra diagonal final limita las coincidencias con el dominio dado y sus subdirectorios. Por ejemplo, ***example.com*** *(****example.com/*** *después del procesamiento) coincide consigo mismo y* ***example.com/search****.*

En las entradas de dominio comodín (entradas con asteriscos o signos de intercalación), la barra inclinada final limita las coincidencias a las URL que se ajustan al patrón especificado. Por ejemplo, para que coincida con la entrada ****.example.com****, una URL debe incluir al menos un subdominio y terminar con el dominio raíz,* ***example.com****. El patrón es:****<subdomain>.example.com****;* ***news.example.com*** *es una coincidencia, pero* ***example.com*** *no lo es porque carece de un subdominio.*

Recomendamos añadir manualmente barras diagonales finales para aclarar el comportamiento de coincidencia previsto de una entrada para cualquiera que la inspeccione. La barra inclinada final es invisible cuando la agrega el cortafuegos.

Los servidores de gestión de Panorama™ que ejecutan PAN-OS® 10.2 solo pueden habilitar esta función para cortafuegos en la misma versión de software. Para habilitar esta función para los cortafuegos que ejecutan PAN-OS 10.1 o anterior, utilice los siguientes comandos de la CLI en cada cortafuegos:

```
admin@PA-850> debug device-server append-end-token on
```

```
admin@PA-850> configure
```

```
admin@PA-850# commit
```

Para deshabilitar esta función, seleccione ***Device (Dispositivo)*** *>* ***Setup (Configuración)*** *>* ***Content-ID (ID del contenido)*** *>* ***URL Filtering (Filtrado de URL)****. A continuación, anule la selección de* ***Append Ending Token (Anexar token de finalización)****. Sin embargo, puede bloquear o permitir el acceso a más URL de las previstas si desactiva esta función. El cortafuegos agrega un asterisco implícito al final de las entradas de dominio que no terminan en / o *. Por ejemplo, si agrega* ***example.com*** *a una lista de URL de sitios web permitidos, el cortafuegos interpreta esa entrada como* ***example.com.****. Como resultado, el cortafuegos permite el acceso a sitios como* ***example.com.domain.xyz****.* Las excepciones de categoría de URL *(PAN-OS 10.1 y anteriores) describen el comportamiento del cortafuegos cuando deshabilita esta función.*

- Las entradas de la lista no distinguen entre mayúsculas y minúsculas.
- Omita `http` y `https` en las entradas de URL.
- Las entradas de URL pueden tener hasta 255 caracteres de longitud.
- Introduzca una *coincidencia exacta* con la dirección IP o la URL que desea bloquear o permitir, o use comodines para crear una *coincidencia de patrón*.

  *Diferentes entradas dan como resultado diferentes coincidencias exactas. Si introduce la URL de una página web específica (**`example.com/contact`**), el cortafuegos limita las coincidencias solo a esa página. La coincidencia exacta para dominios restringe las coincidencias al propio dominio y sus subdirectorios.*
- Considere añadir las URL más utilizadas para acceder a un sitio web o página a su lista de excepciones (por ejemplo, **`blog.paloaltonetworks.com`** y **`paloaltonetworks.com/blog`**) si se puede acceder a la entrada original desde más de una URL.
- La entrada **`example.com`** es distinta de **`www.example.com`**. El nombre de dominio es el mismo, pero la segunda entrada contiene el subdominio *www*.

Palo Alto Networks no admite el uso de expresiones regulares en categorías de URL personalizadas o entradas de listas dinámicas externas. Debe conocer las URL específicas o crear los patrones de URL que desea hacer coincidir utilizando comodines y los siguientes caracteres: `. /? & = ; +`.

Pautas de comodines para las listas de excepción de categoría de URL

Puede utilizar asteriscos (*) y signos de intercalación (^) en las listas de excepciones de categorías de URL para configurar una sola entrada para que coincida con varios subdominios, dominios, dominios de nivel superior (TLD) o páginas sin especificar las URL exactas.

Cómo usar los comodines (asteriscos (*) y símbolos de intercalación (^))

Los siguientes caracteres son separadores de tokens: `. /? & = ; +`. Cada cadena separada con uno o dos de estos caracteres es un token. Utilice caracteres comodines como marcadores de posición de token para indicar que un token específico puede contener cualquier valor. En la entrada **`docs.paloaltonetworks.com`**, los tokens son “docs”, “paloaltonetworks” y “com”.

La siguiente tabla describe cómo funcionan los asteriscos y los signos de intercalación y proporciona ejemplos.

*	^
Indica uno o más subdominios variables, dominios, TLD o subdirectorios. Puede usar un asterisco después de una barra diagonal, por ejemplo, **`example.com/*`**. Por. ej.,: **`*.dominio.com`** coincide con **`docs.dominio.com`** y **`abc.xyz.dominio.com`**.	Indica un subdominio variable, dominio raíz o TLD. No se puede usar el signo de intercalación después de la barra inclinada final. La siguiente entrada no es válida: **`example.com/^`**.

*	^
	Por ej.,: **^.dominio.com** coincide con **docs.dominio.com** y **blog.dominio.com**.

Punto clave: Los asteriscos coinciden con una mayor variedad de URL que los signos de intercalación. Un asterisco corresponde a cualquier número de tokens consecutivos, mientras que un signo de intercalación corresponde exactamente a un token.

Una entrada como **xyz.*.com** coincide con una mayor cantidad de sitios que **xyz.^.^.com**; **xyz.*.com** coincide con sitios con cualquier número de tokens entre las cadenas, y **xyz.^.^.com** coincide con sitios con exactamente dos tokens.

- Un comodín debe ser el **único** carácter dentro de un token. Por ejemplo, **example*.com** es una entrada no válida porque **example** y * están en el mismo token. Sin embargo, una entrada puede contener comodines en más de un token.
- Puede usar asteriscos y signos de intercalación en la misma entrada (por ejemplo, ***.ejemplo.^**).

No cree una entrada con asteriscos (*) consecutivos o entradas con más de nueve símbolos de intercalación (^) consecutivos; este tipo de entradas afectan negativamente al rendimiento del cortafuegos.

*Por ejemplo, no añada una entrada como **mail.*.*.com**. En su lugar, según el rango de sitios web a los que desee controlar el acceso, introduzca **correo.*.com** o **correo.^.^.com**.*

Lista de excepciones de categorías de URL: ejemplos

La siguiente tabla muestra entradas de lista de URL de ejemplo, sitios coincidentes y explicaciones del comportamiento coincidente cuando el cortafuegos añade automáticamente barras inclinadas.

Las entradas en esta tabla no contienen una barra inclinada final para reflejar que el cortafuegos añade una a las entradas correspondientes en segundo plano. Además, las listas de excepciones pueden contener entradas añadidas antes de la guía de barra inclinada final. Excepciones de categoría URL: ejemplos (PAN-OS 10.1) muestra un comportamiento coincidente cuando el cortafuegos no añade barras inclinadas de forma predeterminada.

Recomendamos añadir manualmente barras diagonales finales para aclarar el comportamiento de coincidencia previsto de una entrada para cualquiera que la inspeccione. La barra inclinada final es invisible si la añade el cortafuegos.

Entrada de la lista de excepción de URL	Sitios que coinciden	Explicación
Conjunto de ejemplos 1		
paloaltonetworks.com	paloaltonetworks.com paloaltonetworks.com/network-security/security-subscriptions	El cortafuegos añade una barra diagonal final a la entrada, limitando las coincidencias al dominio exacto y sus subdirectorios.
paloaltonetworks.com/example	paloaltonetworks.com/example	El cortafuegos no añade una barra inclinada final a esta entrada porque el **`ejemplo`** del subdirectorio sigue al dominio. Cuando introduce la URL de una página web específica, el cortafuegos aplica la acción de excepción a la página web especificada.
Conjunto de ejemplo 2: asteriscos		
*.example.com	www.example.com docs.example.com support.tools.example.com	El asterisco expande las coincidencias a todos los subdominios de **`example.com`**. El cortafuegos añade una barra inclinada final a la entrada, excluyendo las coincidencias a la derecha de **`example.com`**, el dominio raíz.
mail.example.* *Esta entrada produce las mismas coincidencias con o sin la función de barra inclinada al final habilitada.*	mail.example.com mail.example.co.uk mail.example.com/#inbox	El asterisco expande las coincidencias a cualquier URL que siga al patrón **`mail.example.<TLD>`**
example.*.com	example.yoursite.com example.es.domain.com	El asterisco expande las coincidencias a las URL donde el subdominio más a

Entrada de la lista de excepción de URL	Sitios que coinciden	Explicación
	example.abc.xyz.com	la izquierda es **example** y el dominio de nivel superior es **com**. La barra diagonal excluye las coincidencias a la derecha del TLD.
example.com/*	example.com/photos example.com/blog/latest cualquier subdirectorio example.com	El dominio va seguido de / y un asterisco, lo que indica que debe haber un subdirectorio. El asterisco sirve como marcador de posición de token para cualquier subdirectorio **example.com**. El cortafuegos no añade una barra diagonal final porque la entrada termina en un asterisco.
Conjunto de ejemplo 3: signos de intercalación		
google.^	google.com google.info	El signo de intercalación expande las coincidencias a las URL que comienzan con

Entrada de la lista de excepción de URL	Sitios que coinciden	Explicación
Los patrones como example.co.^ se utilizan normalmente para hacer coincidir dominios específicos de países, como ***example.co.jp****. Sin embargo, los dominios genéricos de nivel superior (gTLD) generan patrones como example.co.^ que coincide con example.co.info o example.co.amzn, que pueden no pertenecer a la misma organización.*	google.com/search?q=paloaltonetworks	**google** y terminan en un solo TLD. La barra inclinada final excluye las coincidencias a la derecha del último token.
^.google.com	www.google.com noticias.google.com	El signo de intercalación expande las coincidencias a los subdominios de un solo nivel de **google.com**. El cortafuegos añade una barra diagonal final a la entrada, excluyendo las coincidencias a la derecha del dominio raíz.
^.^.google.com	www.maps.google.com support.tools.google.com	Los dos signos de intercalación expanden las coincidencias con las URL que incluyen dos subdominios consecutivos antes de **google.com**. El cortafuegos añade una barra diagonal final a la entrada, excluyendo las coincidencias a la derecha del dominio raíz.

Entrada de la lista de excepción de URL	Sitios que coinciden	Explicación
google.^.com	google.example.com google.company.com	El signo de intercalación expande las coincidencias a las URL donde **`google`** es el subdominio más a la izquierda, seguido de un token y **`.com`**. El cortafuegos añade una barra diagonal final a la entrada, excluyendo las coincidencias a la derecha del TLD.

Creación de una categoría de URL personalizada

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Puede crear una categoría de URL personalizada para definir excepciones a la aplicación de categorías de URL o definir una nueva categoría de URL a partir de varias categorías.

Definir excepciones a la Aplicación de categorías de URL (lista de URL)

Especifique una lista de direcciones URL (agrupadas en una sola categoría personalizada) que desee aplicar independientemente de su Categorías de URL predefinidas. Puede controlar el acceso a esta categoría en un perfil de URL Filtering que aplique a las reglas de la política de seguridad o usar la categoría como criterio de coincidencia en las reglas de la política de seguridad. Por ejemplo, puede bloquear la categoría de URL de redes sociales `social-networking` pero permitir el acceso a LinkedIn.

Definir una categoría de URL personalizada basada en varias categorías PAN-DB (coincidencia de categoría)

Cree una nueva categoría para orientar la aplicación de sitios web o páginas que coincidan con *todas* las categorías definidas como parte de la categoría personalizada. Por ejemplo, PAN-DB podría clasificar un blog de desarrollador que sus ingenieros utilizan para la investigación como `sitios y blogs personales`, `información de computadora e Internet` y `alto riesgo`. Para permitir que los ingenieros accedan al blog y sitios web similares y obtengan

visibilidad de estos sitios web, puede crear una categoría de URL personalizada basada en las tres categorías y establecer el acceso al sitio para que la categoría alerte en un perfil de filtrado de URL.

PAN-DB evalúa las URL con respecto a las categorías de URL personalizadas antes de las listas dinámicas externas y las categorías de URL predefinidas. En consecuencia, el cortafuegos aplica las reglas de la política de seguridad para una URL en una lista de URL personalizada sobre las reglas de la política asociadas con las categorías de URL individuales en las que existe.

Si varias reglas de la política de seguridad incluyen una categoría de URL personalizada, el cortafuegos aplica la regla de la política de seguridad con la acción de perfil de URL Filtering más estricta para el tráfico coincidente.

- Strata Cloud Manager
- PAN-OS y Panorama

Crear una categoría de URL personalizada (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)** > **Access Control (Control de acceso)**.

STEP 2 | En Categorías de URL personalizadas, seleccione **Add Category (Añadir categoría)**.

Introduzca un **Name (Nombre)** descriptivo para la categoría.

STEP 3 | Establezca el **Type (Tipo)** de categoría de URL personalizada en **URL List (Lista de URL)** o **Category Match (Coincidencia de categoría)**.

- **URL List (Lista de URL)**: utilice este tipo de lista para añadir URL que desea aplicar de forma diferente a la categoría de URL a la que pertenecen o para definir una lista de URL como pertenecientes a una categoría personalizada. Consultar las Directrices para las excepciones de categoría de URL a medida que crea entradas de lista de URL.
- **Category Match (Coincidencia con categoría)**: especifique la aplicación a los sitios web que coincidan con un conjunto de categorías. Las páginas o los sitios web deben coincidir con *todas* las categorías definidas en la categoría personalizada.

STEP 4 | En **Items (Elementos)**, seleccione **Add (Añadir)** URL o categorías existentes.

STEP 5 | Seleccione **Save (Guardar)** la categoría de URL personalizada.

STEP 6 | Defina las configuraciones de acceso al sitio y envío de credenciales de usuario para la categoría de URL personalizada.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)** > **URL Access Management Profiles (Perfiles de gestión de acceso URL)**.
2. Seleccione un perfil existente para modificarlo o haga clic en **Add Profile (Añadir perfil)**.
3. En Control de acceso, seleccione la categoría de URL personalizada que creó anteriormente. Se encuentra debajo de `Categorías de URL personalizadas` y encima de `Categorías predefinidas`.
4. Establezca **Site Access (Acceso al sitio)** para la categoría.
5. Establezca **User Credential Submissions (Envíos de credenciales de usuario)** para la categoría.
6. Seleccione **Save (Guardar)** el perfil.

STEP 7 | Aplique el perfil de Gestión de acceso URL a una regla de la política de seguridad.

Un perfil de gestión de acceso URL solo está activo cuando se incluye en un grupo de perfiles al que hace referencia una regla de la política de seguridad.

Siga los pasos para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad). No olvide **Push Config (Enviar configuración)**.

*También puede utilizar categorías de URL personalizadas como criterio de coincidencia de reglas de la política de seguridad. En este escenario, no se define el acceso al sitio para la categoría de URL en un perfil de filtrado de URL. En su lugar, después de crear una categoría de URL personalizada, seleccione la regla de la política de seguridad a la que desea añadir la categoría de URL personalizada [**Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)**]. En **Applications, Services and URLs (Aplicaciones, Servicios y URL)** y Entidades de categoría de URL, haga clic en **Add URL Categories (Añadir categorías de URL)**. Seleccione la categoría de URL personalizada que creó y luego seleccione **Save (Guardar)** la regla de la política de seguridad.*

Crear una categoría de URL personalizada (PAN-OS y Panorama)

STEP 1 | Seleccionar **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)**.

STEP 2 | **Añada** o modifique una categoría de URL personalizada y asígnele un nombre descriptivo en **Name (Nombre)**.

STEP 3 | Configure **Type (Tipo)** en **URL List (Lista de URL)** o en **Category Match (Coincidencia con categoría)**:

- **URL List (Lista de URL)**: añada las URL a las que desea aplicar medidas distintas de las que corresponden a su categoría. Use este tipo de lista para definir las excepciones a la aplicación de las categorías de URL o para definir la lista de URL que pertenecen a

una categoría personalizada. Consulte Excepciones de categoría de URL para obtener instrucciones sobre la creación de entradas de lista de direcciones URL.

*De forma predeterminada, el cortafuegos anexa automáticamente una barra diagonal final (/) a las entradas de dominio (**example.com**) que no terminan en una barra diagonal final o un asterisco (*). La barra diagonal final impide que el cortafuegos asuma un asterisco implícito a la derecha del dominio. En las entradas de dominio que no son comodines, la barra diagonal final limita las coincidencias con el dominio dado y sus subdirectorios. Por ejemplo, **example.com** (**example.com/** después del procesamiento) coincide consigo mismo y **example.com/search**.*

*En las entradas de dominio comodín (entradas que usan asteriscos o intercalaciones), la barra diagonal final limita las coincidencias con las direcciones URL que se ajustan al patrón especificado. Por ejemplo, para que coincida con la entrada ***.example.com**, una URL debe comenzar estrictamente con uno o más subdominios y terminar con el dominio raíz, **example.com**; **news.example.com** es un partido, pero **example.com** no es porque carezca de un subdominio.*

Recomendamos añadir manualmente barras diagonales finales para aclarar el comportamiento de coincidencia previsto de una entrada para cualquier persona que inspeccione su lista de URL. La barra inclinada final es invisible si la añade el cortafuegos. Excepciones de categoría de URL describe la barra diagonal final y el comportamiento de coincidencia con más detalle.

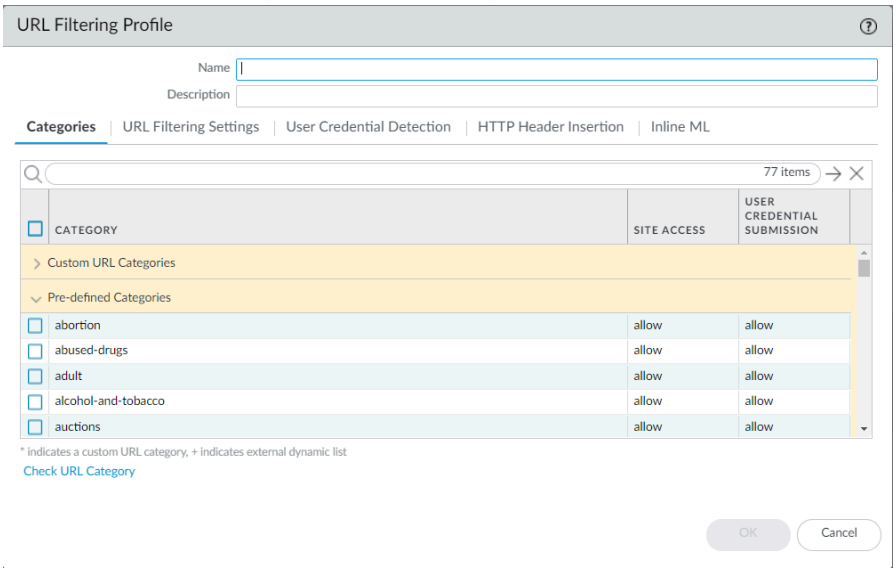
*Para deshabilitar esta función, vaya a **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **URL Filtering (Filtrado de URL)**. A continuación, anule la selección de **Append Ending Token (Anexar token de finalización)**. Si deshabilita esta función, puede bloquear o permitir el acceso a más URL de las previstas. Las excepciones de categoría de URL (PAN-OS 10.1 y anteriores) describen el comportamiento del cortafuegos cuando esta función está deshabilitada.*

- **Category Match (Coincidencia con categoría)**: especifique la aplicación a los sitios web que coincidan con un conjunto de categorías. Las páginas o los sitios web deben coincidir con *todas* las categorías definidas en la categoría personalizada.

STEP 4 | Haga clic en **OK (Aceptar)** para guardar la categoría de URL personalizada.

STEP 5 | Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** o modificar un perfil de filtrado de URL.

La nueva categoría personalizada se muestra en **Categorías de URL personalizadas**:



STEP 6 | Decida las medidas que desea aplicar a la categoría de URL personalizada en **Site Access (Acceso a sitios)** y **User Credential Submission (Envío de credenciales de usuarios)**. (Para controlar los sitios a los que los usuarios pueden enviar sus credenciales corporativas, consulte Prevención del suplantación de credenciales).

STEP 7 | Vincule el perfil de filtrado de URL a una regla de la política de seguridad para aplicarlo al tráfico que coincida con ella.

Seleccione **Policies (Políticas)** > **Security (Seguridad)** > **Actions (Acciones)** y especifique la regla de la política de seguridad para aplicar el tráfico según el perfil de URL Filtering que acaba de actualizar. No olvide hacer clic en **Commit (Confirmar)** para aceptar los cambios.

*Si emplea las categorías de URL personalizadas como criterios de coincidencia con regla de la política de seguridad, En este caso, no se define el acceso al sitio para la categoría URL en un perfil de filtrado de URL. Después de crear una categoría personalizada, vaya a la regla de la política de seguridad a la que desea añadir la categoría de URL personalizada [**Policies (Políticas)** > **Security (Seguridad)**]. Luego, seleccione **Service/URL Category (Servicio/Categoría de URL)** para usar la categoría de URL personalizada como criterio de coincidencia con la regla.*

Usar una lista dinámica externa en un perfil de filtro de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:***

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Una lista dinámica externa es un archivo de texto que está alojado en un servidor web externo. Puede usar esta lista para importar URL y aplicar la política en estas URL. El cortafuegos importa dinámicamente la lista en el intervalo configurado y aplica la política para las URL (se ignorarán las direcciones IP o los dominios) de la lista. Cuando se actualiza la lista en el servidor web, el cortafuegos recupera los cambios y aplica la política a la lista modificada sin necesidad de una confirmación en el cortafuegos.

Para proteger su red de amenazas y malware recientemente detectados, puede usar listas dinámicas externas en los perfiles de filtrado de URL. Para ver directrices sobre el formato de las URL, consulte Directrices para las excepciones de categoría de URL.

- Strata Cloud Manager
- PAN-OS y Panorama

Usar una lista dinámica externa en un perfil de URL Filtering(Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Habilite Prisma Access para hacer referencia a una lista dinámica externa.

Una lista dinámica externa le permite definir una lista importada de direcciones IP, las URL o nombres de dominio que puede usar en las reglas de la política para bloquear o permitir tráfico.

Para configurar una lista dinámica externa, vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)**:

- Asegúrese de que la lista no incluya direcciones IP o nombres de dominio el cortafuegos omite las entradas que no sean URL.
- Utilice las pautas de la lista de URL personalizadas para comprobar el formato de la lista.
- Especifique el **List Type (Tipo de lista)** como **URL List (Lista URL)**.

STEP 2 | Utilice la lista dinámica externa con filtrado de URL.

Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.

- Especifique el **Site Access (Acceso al sitio)** para las URL de la lista dinámica externa.
- Excluya las URL de la lista dinámica externa de la categorización en línea avanzada.

También puede utilizar listas dinámicas externas para crear categorías de URL personalizadas (vuelva al panel de control de gestión de acceso a URL para hacerlo).

Si una URL incluida en una lista dinámica externa también está incluida en una categoría de URL personalizada o en una lista de permitidos o bloqueo; la acción especificada en la categoría personalizada tiene prioridad sobre la lista dinámica externa.

STEP 3 | Compruebe que la acción de política esté forzada.

1. Vea las entradas de la lista dinámica externa [**Manage (Gestionar)** > **Configuration (Configuración)** > **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)**] e intente acceder a una URL de la lista.
2. Verifique que la acción que definió se haya aplicado en el navegador.

Usar una lista dinámica externa en un perfil de filtrado de URL (PAN-OS y Panorama)

STEP 1 | Configure el cortafuegos para acceder a una lista dinámica externa.

- Asegúrese de que la lista no incluya direcciones IP o nombres de dominio el cortafuegos omite las entradas que no sean URL.
- Utilice las pautas de la lista de URL personalizadas para comprobar el formato de la lista.
- Seleccione **URL List (Lista de URL)** de la lista desplegable Type (Tipo).

STEP 2 | Use la lista dinámica externa en un perfil de filtro de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**.
2. Seleccione **Add (Añadir)** para añadir o modifique un perfil de filtro de URL existente.
3. Asigne un nombre al perfil en **Name (Nombre)** y en la pestaña **Categories (Categorías)**, seleccione la lista dinámica externa en la lista de categorías.
4. Haga clic en Action (Acción) para seleccionar una acción más detallada para las URL en la lista dinámica externa.

   Si una URL incluida en una lista dinámica externa también está incluida en una categoría de URL personalizada o en una lista de permitidos o bloqueo; la acción especificada en la categoría personalizada tiene prioridad sobre la lista dinámica externa.
5. Haga clic en **OK (Aceptar)**.
6. Adjunte el perfil de filtrado de URL a una regla de la política de seguridad.
   1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
   2. Seleccione la pestaña **Actions (Acciones)** y, en la sección Profile Setting (Ajuste de perfil), seleccione el nuevo perfil en el menú desplegable **URL Filtering (Filtrado de URL)**.
   3. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

STEP 3 | Compruebe que la acción de política esté forzada.

1. Visualice las entradas de la lista dinámica externa e intente acceder a la URL desde la lista.
2. Verifique que la acción que definió se haya aplicado en el navegador.
3. Para supervisar la actividad del cortafuegos:
   1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de la red y la actividad bloqueada para la URL a la cual accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)** para acceder a la vista detallada del log.

STEP 4 | Verifique si las entradas en la lista dinámica externa se ignoraron u omitieron.

En una lista de tipo URL, el cortafuegos omite las entradas que no son URL como no válidas e ignora las entradas que superan el límite máximo del modelo de cortafuegos.

*Para comprobar si alcanzó el límite de un tipo de lista dinámica externa, seleccione **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)** y haga clic en **List Capacities (Capacidades de la lista)**.*

Use el siguiente comando CLI en un cortafuegos para revisar los detalles de una lista.

```
request system external-list show type url name <list_name>
```

Por ejemplo:

```
request system external-list show type url name My_URL_List vsys5/
My_URL_List: Próxima actualización en: Mar Jan 3 14:00:00 2017
 Fuente: http://example.com/My_URL_List.txt Con referencia: Sí
 Válido: Sí Auth-Valid: Sí Total de entradas válidas: 3 Total de
 entradas no válidas: 0 URL válidas: www.URL1.com www.URL2.com
 www.URL3.com
```


Prácticas recomendadas de filtrado de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

La solución de filtrado de URL de Palo Alto Networks le protege de las amenazas basadas en la web y le proporciona una forma sencilla de supervisar y controlar la actividad web. Para aprovechar al máximo tu implementación del filtrado de URL, primero cree reglas permitidas para las aplicaciones en las que confía para desarrollar su actividad empresarial. A continuación, revise las categorías de URL que clasifican el contenido malicioso y de exploits; le recomendamos que las bloquee directamente. Después, para todo lo demás, estas prácticas recomendadas pueden servirle como guía sobre cómo reducir la exposición a las amenazas basadas en la web sin limitar el acceso de sus usuarios al contenido web que necesitan.

- Antes de comenzar, identifique las aplicaciones que desee permitir y cree las reglas de permiso de aplicaciones como parte de la creación de una política de seguridad de puerta de enlace de Internet recomendada.

  Las aplicaciones permitidas incluyen no solo las aplicaciones que usted suministra y administra para fines empresariales y de infraestructura, sino también otras aplicaciones que los usuarios pueden necesitar para desempeñar sus funciones, y las aplicaciones que usted puede elegir autorizar para uso personal.

  Una vez que haya identificado estas aplicaciones autorizadas, puede usar el filtrado de URL para controlar y proteger toda la actividad web que no esté en la lista de permisos.
- Obtenga visibilidad de la actividad web de sus usuarios para poder planificar la política de filtrado de URL de la manera más eficaz para su organización. Esto incluye lo siguiente:
  - Uso de Test A Site (Probar un sitio) para ver cómo PAN-DB, la base de datos de la nube de filtrado de URL de Palo Alto Networks, clasifica una URL específica y para conocer todas las categorías de URL posibles.
  - Empiece por un perfil pasivo (sobre todo) de filtrado de URL que alerte sobre las categorías de URL. Así obtiene visibilidad sobre los sitios a los que acceden los usuarios y puede decidir cuáles permitir, limitar y bloquear.
  - Supervisión de la actividad web para evaluar los sitios a los que acceden sus usuarios y ver cómo se alinean con las necesidades de su empresa.

- Bloquee las categorías de URL que clasifiquen contenido web malicioso y de vulnerabilidades. Aunque sabemos que estas categorías son peligrosas, siempre tenga en cuenta que las categorías de URL que decida bloquear pueden depender de las necesidades de su empresa.
- Use categorías de URL para descifrar gradualmente y para excluir información confidencial o personal (como servicios financieros y salud y medicina) del descifrado.

  Planifique descifrar primero el tráfico más peligroso (las categorías de URL con mayor probabilidad de tener tráfico malicioso, como los juegos o de alto riesgo) y luego, descifre más a medida que gane experiencia. Como alternativa, descifre primero las categorías de URL que no afecten a su empresa (si algo no funciona, no afectará a la empresa), por ejemplo, las fuentes de noticias. En ambos casos, descifre algunas categorías de URL, escuche los comentarios del usuario, ejecute informes para garantizar que el descifrado funciona según lo esperado y, luego, descifre de manera gradual algunas categorías de URL más y así sucesivamente. Planifique excluir sitios de descifrado si no puede descifrarlos por motivos técnicos o porque decide no hacerlo.

  El descifrado limitado basado en categorías de URL también es una práctica recomendada para el descifrado.
- Prevenga el robo de credenciales mediante la habilitación del cortafuegos, la detección de envíos de credenciales corporativas a los sitios y el control de esos envíos según la categoría de URL. Bloquee a los usuarios para el envío de credenciales a sitios malintencionados y no fiables, advierta a los usuarios sobre el ingreso de credenciales corporativas en sitios desconocidos o la reutilización de credenciales corporativas en sitios no corporativos, y permita explícitamente a los usuarios que envíen credenciales a sitios corporativos y aprobados.
- Bloquee variantes maliciosas de exploits de JavaScript y ataques de phishing en tiempo real. La habilitación de la categorización local en línea le permite analizar páginas web de forma dinámica mediante el aprendizaje automático en el cortafuegos.
- Configurar la categorización en línea para permitir que motores de detección basados en aprendizaje profundo y aprendizaje automático en línea analicen el contenido de páginas web sospechosas y protejan a los usuarios frente a ataques web de día cero. La categorización en línea en la nube es capaz de detectar y prevenir ataques de phishing avanzados y dirigidos, y otros ataques basados en la web que utilizan técnicas de evasión avanzadas, como encubrimiento, ataques de varios pasos, desafíos de CAPTCHA y direcciones URL de un solo uso nunca antes vistas.
- Descifre, inspeccione y limite estrictamente la forma en que los usuarios interactúan con contenido de riesgo alto y medio (si decidió no bloquear ninguno de las categorías de URL maliciosas por razones empresariales, también deberá limitar estrictamente la forma en que los usuarios interactúan con ellas).

  El contenido web que sancione y las categorías de URL maliciosas que bloquee directamente son solo una parte de su tráfico web general. El resto del contenido al que acceden sus usuarios es una combinación de contenido benigno (riesgo bajo) y de riesgo (alto riesgo alto y medio). El contenido de riesgo alto y medio no se confirma como malicioso, pero está estrechamente relacionado con sitios que sí lo son. Por ejemplo, una URL de alto riesgo podría estar en el mismo dominio que un sitio web malicioso o quizás haber alojado contenido malicioso en el pasado.

  Sin embargo, muchos sitios que representan un riesgo para su empresa también proporcionan recursos y servicios valiosos a sus usuarios (los servicios de almacenamiento en la nube son un

buen ejemplo). Aunque estos recursos y servicios son necesarios para las empresas, también es más probable que se utilicen como parte de un ciberataque. A continuación, le mostramos cómo controlar la forma en la que interactúan los usuarios con ese contenido potencialmente peligroso, a la vez que les proporciona una buena experiencia de usuario:

- En un perfil de filtrado de URL, configure las categorías de riesgo alto y medio en **continue (Continuar)** para ver la página de respuesta en la que se advierte a los usuarios que están visitando un sitio potencialmente peligroso. Indíqueles cómo tomar precauciones si deciden continuar en el sitio. Si no desea solicitar a los usuarios una página de respuesta, alerte sobre las categorías de riesgo alto y medio.
- Decrypt (Descifrar) permite descifrar sitios de riesgo alto y medio.
- Siga las prácticas recomendadas sobre antispyware, protección frente a vulnerabilidades y el bloqueo de archivos para sitios de riesgo alto y medio. Una posible medida de protección consiste en impedir la descarga de tipos de archivos peligrosos y bloquear el código JavaScript oculto.
- Prevenga el robo de credenciales impidiendo que los usuarios envíen sus credenciales corporativas a los sitios de riesgo medio y alto.

- Las escuelas o las instituciones académicas deben usar la aplicación segura de la búsqueda para asegurarse de que los motores de búsqueda filtren las imágenes y vídeos para adultos de los resultados de búsqueda.
- Mantenga las solicitudes web iniciales durante la búsqueda de la categoría URL.

  Cuando un usuario visita un sitio web, Advanced URL Filtering comprueba las categorías de URL almacenadas en caché para categorizar el sitio. Si no encuentra la categoría de la URL en el caché, este realizará una búsqueda en PAN-DB, la base de datos de URL de Palo Alto Networks. De forma predeterminada, la solicitud web del usuario se permite durante esta búsqueda en la nube.

  Sin embargo, si elige retener solicitudes web, puede bloquear la solicitud hasta que Advanced URL Filtering encuentre la categoría de URL o agota el tiempo de espera. Si se agota el tiempo de búsqueda, el cortafuegos considera que la categoría de URL no está resuelta. Busque esta función en la configuración de Filtrado de URL, **Hold client request for category lookup (Retener solicitud de cliente para búsqueda de categoría)**.

Prueba de la configuración de filtrado de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Para probar las configuraciones de políticas de su filtrado de URL, utilice las páginas de prueba de filtrado de URL de Palo Alto Networks. Estas páginas se han creado para la prueba segura de todas las categorías URL predefinidas y Advanced URL Filteringcategorías de detección en tiempo real.

se puede acceder a las páginas de prueba a través de conexiones HTTP y HTTPS. Sin embargo, debe habilitar el descifrado SSL para ver las páginas de prueba a través de HTTPS.

Puede verificar la clasificación de un sitio web específico utilizando la herramienta de búsqueda de categorías de URL de Palo Alto Networks, Test A Site.

Siga el procedimiento correspondiente a su suscripción de filtrado de URL.

Verificación del URL Filtering

Si tiene una suscripción heredada a filtrado de URL, pruebe y compruebe que el cortafuegos clasifica, aplica y registra correctamente las direcciones URL de las categorías a las que acceden los usuarios finales.

STEP 1 | Acceda a un sitio web en la categoría URL de interés.

Considere la posibilidad de probar sitios en categorías de URL bloqueadas. Puede utilizar una página de prueba (urlfiltering.paloaltonetworks.com/test-<*url-category*>) para evitar acceder directamente a un sitio. Por ejemplo, para probar su política de bloqueo de malware, visite https://urlfiltering.paloaltonetworks.com/test-malware.

STEP 2 | Revise los logs de filtrado de URL y tráfico para comprobar que el cortafuegos procesa el sitio correctamente.

Por ejemplo, si configuró una página de bloqueo para que se muestre cuando alguien acceda a un sitio que infrinja la política de su organización, compruebe que aparezca cuando visite el sitio de prueba.

Verificar Advanced URL Filtering

Si tiene una suscripción a Advanced URL Filtering, pruebe y verifique que las URL enviadas al Advanced URL Filtering se analizan correctamente.

Palo Alto Networks recomienda configurar los ajustes de acción de detección en tiempo real (categorización en línea en la nube) en ***alert (alertar)*** *para sus perfiles de filtrado de URL activos. Esto proporciona visibilidad de las URL analizadas en tiempo real y bloqueará (o permitirá, según la configuración de la política) en función de la configuración de categoría establecida para amenazas web específicas.*

El cortafuegos aplica la acción más grave de las acciones configuradas para las categorías de URL detectadas de una URL determinada. Por ejemplo, supongamos que example.com se clasifica como detección en tiempo real, comando y control y compras: categorías con una acción de alerta, bloqueo y permitir configurada, respectivamente. El cortafuegos bloquea la URL porque el bloqueo es la acción más grave de las categorías detectadas.

STEP 1 | Visite cada una de las siguientes direcciones URL de prueba para comprobar que el servicio de Advanced URL Filtering está clasificando correctamente las direcciones URL:

- **Malware**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-malware
- **Phishing**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-phishing
- **C2**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-command-and-control
- **Grayware**—http://urlfiltering.paloaltonetworks.com/test-inline-url-analysis-grayware

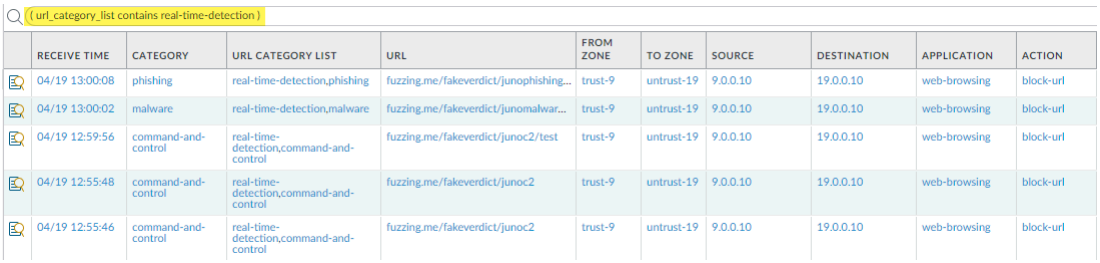
Si está habilitada la categorización en línea en la nube, utilice las siguientes URL para probar el funcionamiento de la característica:

- **Malware**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-malware
- **Phishing**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
- **Grayware**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-grayware
- **Estacionado**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-parked
- **Adulto**—http://urlfiltering.paloaltonetworks.com/test-inline-content-analysis-adult

STEP 2 | Supervisar la actividad web para comprobar que Advanced URL Filtering ha clasificado correctamente las URL de prueba:

1. Filtre sus logs de filtrado de URL utilizando lo siguiente: `(url_category_list contains real-time-detection)`.

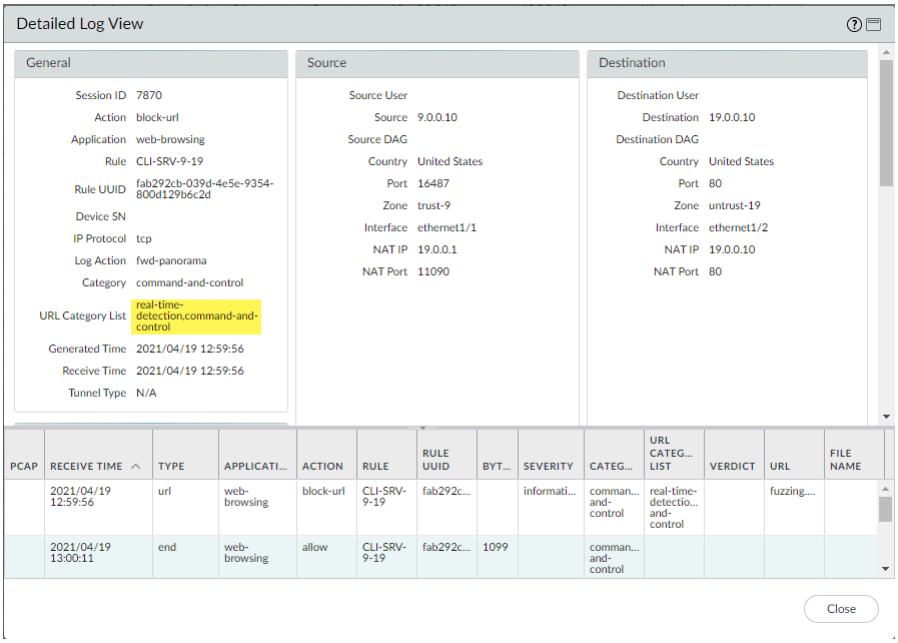
   También se muestran coincidencias de categorías de páginas web adicionales, estas corresponden a las categorías definidas por PAN-DB.



	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	URL	FROM ZONE	TO ZONE	SOURCE	DESTINATION	APPLICATION	ACTION
	04/19 13:00:08	phishing	real-time-detection,phishing	fuzzing.me/fakeverdict/junophishing...	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
	04/19 13:00:02	malware	real-time-detection,malware	fuzzing.me/fakeverdict/junomalwar...	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
	04/19 12:59:56	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2/test	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
	04/19 12:55:48	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url
	04/19 12:55:46	command-and-control	real-time-detection,command-and-control	fuzzing.me/fakeverdict/junoc2	trust-9	untrust-19	9.0.0.10	19.0.0.10	web-browsing	block-url

2. Eche un vistazo detallado a los registros para verificar que cada tipo de amenaza web se analice y clasifique correctamente.

   En el siguiente ejemplo, la URL se clasifica como analizada en tiempo real y que posee cualidades que la definen como comando y control (C2). Debido a que la categoría C2 tiene una acción más grave asociada que la detección en tiempo real (bloquear en lugar de alerta), la URL se clasifica como comando y control y se bloquea.



Funciones de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Después de configurar los componentes básicos de la implementación del filtrado de URL, considere la posibilidad de configurar las siguientes características:

- Categorización en línea
- Inspección del protocolo de enlace SSL/TLS
- Cancelación de administrador de URL
- Prevención de phishing de credenciales
- Páginas de respuesta de filtrado de URL
- Aplicación de búsquedas seguras
- (Solo Prisma Access) Integración con aislamiento remoto del navegador (RBI)

Inspeccionar los protocolos de enlace SSL/TLS

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Examinar los protocolos de enlace SSL/TLS mejora la seguridad de la red y optimiza las suscripciones heredadas y de Advanced URL Filtering. Cuando habilita la inspección de acceso rápido SSL/TLS, Advanced URL Filtering utiliza los datos en el acceso rápido para identificar el tráfico y hacer cumplir las reglas de la política de seguridad aplicables lo antes posible.

Así es como funciona

Primero, se analiza el Mensaje de bienvenida del cliente en busca del campo *Indicación de nombre del servidor (SNI)*, una extensión de protocolo TLS que contiene el nombre de host de un sitio web solicitado. A continuación, se determina la categoría de URL y el destino del servidor del tráfico a partir del nombre del host. A continuación, el tráfico se impone en función de su categoría de URL. Si se detecta una amenaza, como por ejemplo un servidor web malicioso en el campo SNI, o si una regla de la política de seguridad bloquea el sitio web; el apretón de manos termina y la sesión web finaliza inmediatamente. Si no se detecta ninguna amenaza y se permite el tráfico por política, el protocolo de enlace SSL/TLS se completa y se intercambia datos de la aplicación a través de la conexión segura.

Las páginas de respuesta de filtrado de URL no se muestran para los sitios bloqueados durante las inspecciones de acceso SSL/TLS porque el cortafuegos restablece la conexión HTTPS. El restablecimiento de la conexión finaliza los protocolos de enlace SSL/TLS e impide la notificación del usuario por página de respuesta. El navegador muestra un mensaje de error de conexión estándar.

Los detalles de los protocolos de enlace SSL/TLS y las sesiones realizadas correctamente estarán en los logs de tráfico y descifrado. Los detalles de las sesiones fallidas se pueden encontrar en los logs de filtrado de URL; los logs de descifrado no se generan para las sesiones web bloqueadas durante los protocolos de enlace SSL/TLS.

- Strata Cloud Manager
- PAN-OS y Panorama

Inspeccionar los protocolos de enlace SSL/TLS (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

Un requisito para inspeccionar los protocolos de enlace SSL es que descifre el tráfico SSL/TLS a través del proxy SSL de reenvío o la inspección de SSL entrante.

STEP 1 | Confirme que su licencia de Prisma Access incluye una suscripción de Advanced URL Filtering.

1. Seleccione **Manage (Gestionar)** > **Service Setup (Configuración de servicio)** > **Overview (Descripción general)** y haga clic en el valor de cantidad hipervinculado Aparece información, incluida la de los servicios de seguridad.
2. En Servicios de seguridad, confirme que hay una marca de verificación junto a Filtrado de URL.

STEP 2 | Compruebe que descifra el tráfico SSL/TLS a través de SSL Forward Proxy (Proxy SSL de reenvío) o SSL Inbound Inspection (Inspección de SSL entrante).

STEP 3 | Habilite la inspección de protocolos de enlace SSL/TLS por CTD. Esta opción está deshabilitada por defecto.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **Decryption (Descifrado)**.
2. Por Configuración de descifrado, seleccione el icono de configuración. A continuación, seleccione **Inspect TLS Handshake Messages (Inspeccionar mensajes de protocolo de enlace TLS)**.

   Alternativamente, puede usar el comando de la CLI **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`**.
3. Haga clic en **Save (Guardar)** para guardar sus cambios. En Configuración de descifrado, la configuración del mensaje Inspeccionar protocolo de enlace TLS deberá decir Habilitado.

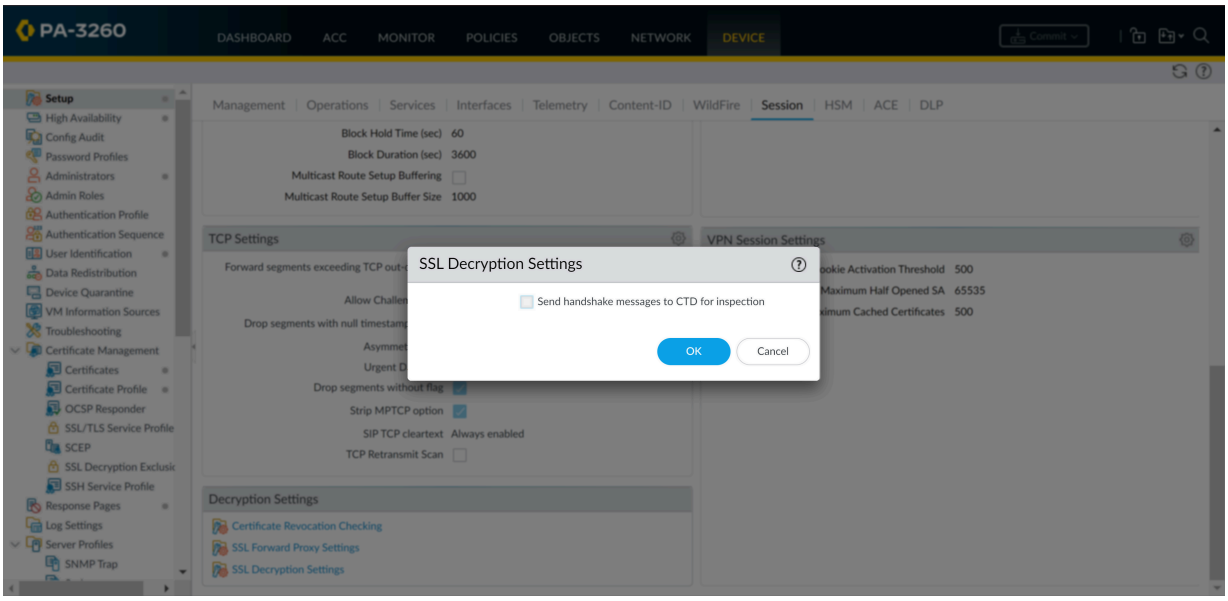
STEP 4 | Seleccione **Push Config (Enviar configuración)** para guardar y confirmar los cambios.

Inspeccionar los protocolos de enlace SSL/TLS (PAN-OS y Panorama)

STEP 1 | Seleccione **Device (Dispositivo) > Licenses (Licencias)** para confirmar que tiene una licencia de Advanced URL Filtering activa o una licencia de filtrado de URL heredada.

STEP 2 | Compruebe que descifra el tráfico SSL/TLS a través de SSL Forward Proxy (Proxy SSL de reenvío) o SSL Inbound Inspection (Inspección de SSL entrante).

STEP 3 | Habilite la inspección de protocolos de enlace SSL/TLS por CTD. De forma predeterminada, la opción está deshabilitada.



1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Session (Sesión)** > **Decryption Settings (Configuración de descifrado)** > **SSL Decryption Settings (Configuración de descifrado SSL)**.
2. Seleccione **Send handshake messages to CTD for inspection (Enviar mensajes del protocolo de enlace a CT para su inspección)**.

   Alternativamente, puede usar el comando de la CLI **`set deviceconfig setting ssl-decrypt scan-handshake <yes|no>`** .
3. Haga clic en **OK (Aceptar)**.

STEP 4 | Haga clic en **Commit (Confirmar)** para aceptar los cambios en la configuración.

Habilitación del acceso a determinados sitios mediante contraseña

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

En algunos casos, puede ser necesario requerir acceso con contraseña a sitios web de ciertas categorías. Por ejemplo, su empresa puede bloquear categorías de URL que amenacen la seguridad y el bienestar de los empleados. Sin embargo, ciertos empleados pueden necesitar acceso a estas categorías para fines legítimos o de investigación. Para equilibrar la seguridad y las necesidades empresariales, la implementación de anulaciones de administrador de URL puede ser una solución eficaz.

Para crear una anulación de administrador de URL, establezca la acción de una categoría en **override (anular)**. Luego, cree una contraseña que los usuarios deben introducir para acceder a los sitios de esta categoría. Cuando los usuarios intentan acceder a un sitio web en una categoría que ha anulado, aparece una Página de respuesta Continuar y anular. Esta página notifica a los usuarios que un sitio web está bloqueado y les pide que introduzcan una contraseña para continuar en el sitio.

- Strata Cloud Manager
- PAN-OS y Panorama

Habilitación del acceso a determinados sitios mediante contraseña (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Vaya al panel de gestión de acceso URL.

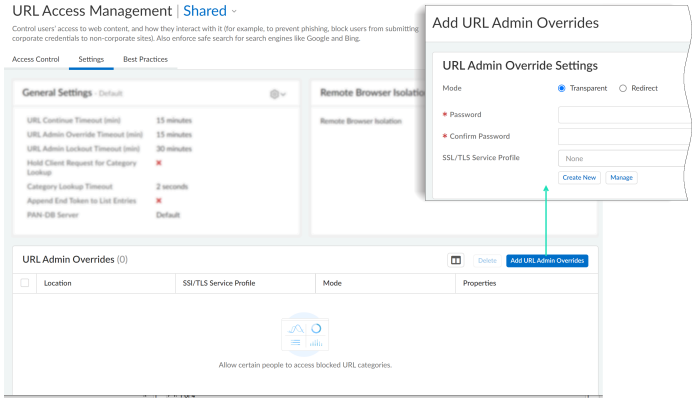
Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.

STEP 2 | Seleccione **Settings**.

STEP 3 | Cree una contraseña de anulación de administrador de URL.

1. Vaya a Anulaciones de administrador de URL y **Add URL Admin Overrides (Añadir anulaciones de administrador de URL)**.
2. (Opcional) Seleccione un **Mode (Modo)** para solicitar a los usuarios la contraseña:
   - **Transparent (Transparente)**: el símbolo de contraseña parece originarse en la URL de destino original. El cortafuegos intercepta el tráfico del navegador destinado a los sitios en una categoría de URL establecida para anular y emite un HTTP 302 para solicitar la contraseña, que se aplica en un nivel por sistema.
   - **Redirect (Redirigir)**: el símbolo de contraseña aparece en una **Address (Dirección)** (dirección IP o nombre de host DNS) que especifique. El cortafuegos intercepta el tráfico HTTP o HTTPS a una categoría de URL establecida para anular y utiliza una redirección HTTP 302 para enviar la solicitud a una interfaz de Capa 3 en el cortafuegos.
3. Introduzca una **Password (Contraseña)** y, a continuación, introdúzcala de nuevo para **Confirm Password (Confirmar contraseña)**.
4. (Opcional) Seleccione un **SSL/TLS Service Profile (Perfil de servicio SSL/TLS)**.

   Puede crear y administrar perfiles de servicio SSL/TLS haciendo clic en **Create New (Crear nuevo)** y **Manage (Gestionar)**, respectivamente.
5. Haga clic en **Save (Guardar)** para guardar sus cambios.



STEP 4 | (Opcional) Establezca la duración de la anulación del acceso y los bloqueos de contraseñas.

De forma predeterminada, los usuarios pueden acceder a sitios web en categorías para las que han introducido correctamente una contraseña de anulación durante 15 minutos. Después de

que pase el intervalo predeterminado o personalizado, los usuarios deben volver a introducir la contraseña.

De forma predeterminada, los usuarios se bloquean durante 30 minutos después de tres intentos fallidos de contraseña. Después de que el usuario se bloquea durante la duración predeterminada o personalizada, puede intentar acceder a los sitios web de nuevo.

1. Personalizar la configuración general.
2. Para **URL Admin Override Timeout (Tiempo de espera de anulación de administrador de URL)**, introduzca un valor (en minutos) del 1 al 86.400.
3. Para **URL Admin Lockout Timeout (Tiempo de espera de bloqueo de administrador de URL)**, introduzca un valor (en minutos) del 1 al 86.400.
4. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 5 | Especifique las categorías de URL que requieren acceso con contraseña.

1. En el panel Gestión de acceso URL, en la pestaña **Access Control (Control de acceso)**, vaya a Perfiles de gestión de acceso URL y modifique o seleccione **Add Profile (Añadir perfil)**.
2. En Control de acceso, seleccione las categorías que requieren acceso con contraseña.
3. Con todas las categorías seleccionadas, haga clic en **Set Access (Establecer acceso)** y, a continuación, seleccione **Override (Anular)**.

   Debería ver que el acceso al sitio para las categorías resaltadas ahora dice `anular`.
4. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 6 | Aplique el perfil de Gestión de acceso URL a una regla de la política de seguridad.

Un perfil de gestión de acceso URL solo está activo cuando se incluye en un grupo de perfiles al que hace referencia una regla de la política de seguridad.

Siga los pasos para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad). Asegúrese de **Push Config (Enviar configuración)** cuando haya terminado.

Habilitación del acceso a determinados sitios mediante contraseña (PAN-OS y Panorama)

STEP 1 | Establezca una contraseña de anulación de administrador de URL.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content ID (ID de contenido)**.
2. En la sección **Anulación de administrador de URL**, haga clic en **Add (Añadir)**.
3. En el campo **Ubicación**, seleccione el sistema virtual al que se aplica esta contraseña.
4. Introduzca una **Password (Contraseña)** y, a continuación, introdúzcala de nuevo para **Confirm Password (Confirmar contraseña)**.
5. Seleccione un **SSL/TLS Service Profile**.

   Perfiles de servicio SSL/TLS especifica el certificado que el cortafuegos presenta al usuario si el sitio con la anulación es un sitio HTTPS.
6. Seleccione el **Mode (Modo)** para indicar al usuario la contraseña:

   - **Transparent (Transparente)**: el símbolo de contraseña parece originarse en la URL de destino original. El cortafuegos intercepta el tráfico del navegador destinado a los sitios en una categoría de URL establecida para anular y emite un HTTP 302 para solicitar la contraseña, que se aplica en un nivel por sistema.

     El explorador del cliente mostrará errores de certificado si no confía en el certificado.
   - **Redirect (Redirigir)**: el símbolo de contraseña aparece en una **Address (Dirección)** (dirección IP o nombre de host DNS) que especifique. El cortafuegos intercepta el tráfico HTTP o HTTPS a una categoría de URL establecida para anular y utiliza una redirección HTTP 302 para enviar la solicitud a una interfaz de Capa 3 en el cortafuegos.
7. Haga clic en **OK (Aceptar)**.

STEP 2 | (Opcional) Establezca la duración de la anulación de acceso y los bloqueos de contraseña.

De forma predeterminada, los usuarios pueden acceder a sitios web en categorías para las que han introducido correctamente una contraseña de anulación durante 15 minutos. Después de que pase el intervalo predeterminado o personalizado, los usuarios deben volver a introducir la contraseña.

De forma predeterminada, los usuarios se bloquean durante 30 minutos después de tres intentos fallidos de contraseña. Después de que el usuario se bloquea durante la duración predeterminada o personalizada, puede intentar acceder a los sitios web de nuevo.

1. Edite la sección Filtrado de URL.
2. Para el **URL Admin Override Timeout (Tiempo de espera de anulación de administrador de URL)**, introduzca un valor (en minutos) de 1 a 86.400. ---Por defecto, los usuarios pueden acceder a sitios dentro de la categoría durante 15 minutos sin volver a introducir la contraseña.
3. Para **URL Admin Lockout Timeout (Tiempo de espera de bloqueo de administrador de URL)**, introduzca un valor (en minutos) del 1 al 86.400.
4. Haga clic en **OK (Aceptar)**.

STEP 3 | (Solo en el modo Redirigir) Cree una interfaz de capa 3 a la que redirigir las solicitudes web para los sitios en una categoría configurada para la anulación.

1. Cree un perfil de gestión para habilitar la interfaz de modo que muestre la página de respuesta de continuación y anulación de filtrado de URL:
   1. Seleccione **Network (Red)** > **Interface Mgmt (Gestión de interfaz)** y haga clic en **Add (Añadir)**.
   2. Introduzca un **Nombre** para el perfil, seleccione **Páginas de respuesta** y, a continuación, haga clic en **Aceptar**.
2. Cree la interfaz de capa 3. Asegúrese de adjuntar el perfil de gestión que acaba de crear (en la pestaña **Advanced [Avanzado]** > **Other Info [Otra información]** del cuadro de diálogo Ethernet Interface [Interfaz Ethernet]).

STEP 4 | (Solo en el modo Redirigir) Para redirigir a los usuarios de forma transparente sin mostrar errores de certificado, instale un certificado que coincida con la dirección IP de la interfaz a la que va a redirigir las solicitudes web para un sitio en una categoría de URL configurada para la anulación. Puede generar un certificado autofirmado o importar un certificado firmado por una CA externa.

Para usar un certificado autofirmado, primero debe crear un certificado de CA raíz y, a continuación, usar esa CA para firmar el certificado que usará para la anulación de administrador de URL del modo siguiente:

1. Para crear un certificado de CA raíz, seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificates (Certificados)** > **Device Certificates (Certificados del dispositivo)** y luego haga clic en **Generate (Generar)**. Introduzca un **Nombre de certificado**, como RootCA. No seleccione ningún valor en el campo **Firmado por** (esto es lo que indica que está autofirmado). Asegúrese de seleccionar la casilla de verificación **Autoridad del certificado** y, a continuación, haga clic en **Generar** para generar el certificado.
2. Para crear el certificado que se usará para la anulación de administrador de URL, haga clic en **Generate (Generar)**. Especifique el **Nombre del certificado** y el nombre de host DNS o la dirección IP de la interfaz como el **Nombre común**. En el campo **Signed By (Firmado por)**, seleccione la CA que creó en el paso anterior. Añada un atributo de dirección IP y especifique la dirección IP de la interfaz de capa 3 a la que redirigirá las solicitudes web para las categorías de URL con la acción de anulación.
3. Seleccione **Generar** el certificado.
4. Para configurar clientes para que confíen en el certificado, seleccione el certificado de CA en la pestaña **Device Certificates (Certificados de dispositivos)** y haga clic en **Export (Exportar)**. A continuación deberá importar el certificado como una CA raíz de confianza en todos los exploradores de cliente, ya sea configurando manualmente el explorador o añadiendo el certificado a las raíces de confianza en un objeto de directiva de grupo (GPO) de Active Directory.

STEP 5 | Especifique qué categorías de URL requieren una contraseña de anulación para permitir el acceso.

1. Seleccione **Objects (Objetos)** > **URL Filtering (Filtrado de URL)** y seleccione un perfil de filtrado de URL existente o seleccione **Add (Añadir)** para añadir uno nuevo.
2. En la pestaña **Categories (Categorías)**, establezca la acción en **override (anular)** para cada categoría que requiera una contraseña.
3. Complete las secciones restantes del perfil de filtrado de URL y, a continuación, haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 6 | Aplique el perfil de filtrado de URL a las reglas de la política de seguridad que permiten el acceso a los sitios que requieren la anulación de la contraseña para el acceso.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y seleccione la política de seguridad adecuada para modificarla.
2. Seleccione la pestaña **Acciones** y, en la sección **Ajuste de perfil**, haga clic en el menú desplegable **Filtrado de URL** y seleccione el perfil.
3. Haga clic en **OK (Aceptar)** para guardar.

STEP 7 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

Prevención de phishing de credenciales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Los sitios de phishing son sitios que los atacantes disfrazan de sitios web legítimos con el objetivo de robar información del usuario, especialmente, las credenciales que proporcionan acceso a su red. Cuando un correo electrónico de phishing entra en una red, solo se necesita que un usuario haga clic en un enlace e introduzca las credenciales para poner en marcha una filtración. Puede detectar y evitar los ataques de phishing en curso, y evitar el robo de credenciales, controlando los sitios que pueden recibir credenciales corporativas basadas en la categoría de URL del sitio de los usuarios. Esto le permite evitar que los usuarios envíen credenciales a sitios no fiables, además de permitir a los usuarios continuar enviando credenciales a sitios corporativos y sancionados.

La prevención de phishing de credenciales funciona mediante el análisis de los envíos de nombres de usuario y contraseñas a sitios web, y la comparación de esos envíos con las credenciales corporativas válidas. Puede seleccionar los sitios web en los que desea permitir o bloquear la recepción de credenciales corporativas en función de la categoría de URL del sitio web. Cuando un usuario intenta enviar credenciales a un sitio de una categoría que ha restringido, una página de respuesta de bloqueo impide que el usuario envíe credenciales o una página de continuación advierte a los usuarios que no envíen credenciales a sitios en determinadas categorías de URL, pero les permite continuar con la transmisión. Puede Personalizar páginas de respuesta para educar a los usuarios frente a la reutilización de credenciales corporativas, incluso en sitios legítimos que no son de phishing.

En los temas a continuación se describen los diferentes métodos de detección de credenciales que puede elegir y se proporcionan instrucciones para configurar la protección frente al phishing de credenciales.

- Métodos para comprobar los envíos de credenciales corporativas
- Configuración de la detección de credenciales con el agente de ID de usuario basado en Windows
- Habilitar la prevención de phishing de credenciales

Métodos para comprobar los envíos de credenciales corporativas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Antes de habilitar la prevención de phishing de credenciales, decida el método que desea utilizar para comprobar si las credenciales que se enviaron a una página web son credenciales corporativas válidas.

Método para comprobar las credenciales enviadas	Requisitos de configuración de User-ID	¿Cómo detecta este método los nombres de usuario o las contraseñas corporativas que los usuarios envían a los sitios web?
Asignación de grupos	Configuración de asignación de grupos en el cortafuegos	El cortafuegos realiza comprobaciones para determinar si el nombre de usuario que un usuario envía a un sitio restringido coincide con cualquier nombre de usuario corporativo válido. Para ello, el cortafuegos compara el nombre de usuario enviado a la lista de nombres de usuario en su tabla de asignación de usuarios a grupos para detectar cuándo los usuarios envían nombres de usuario corporativos a sitios en una categoría restringida. Este método sólo comprueba envíos de nombre de usuario corporativo basándose en la pertenencia a un grupo LDAP, lo que hace que sea sencillo de configurar, pero más propenso a falsos positivos.
Asignación de direcciones IP a usuarios	Asignaciones de direcciones IP a nombres de usuario identificadas mediante la asignación de usuarios, GlobalProtect	El cortafuegos realiza una comprobación para determinar si el nombre de usuario que un usuario envía a un sitio restringido se asigna a la dirección IP del nombre de usuario de inicio de sesión. Para ello, el cortafuegos compara la dirección IP del nombre de usuario de inicio de sesión y el nombre de usuario enviado a un sitio web con la tabla de asignación de direcciones IP a usuarios para detectar

Método para comprobar las credenciales enviadas	Requisitos de configuración de User-ID	¿Cómo detecta este método los nombres de usuario o las contraseñas corporativas que los usuarios envían a los sitios web?
	o la Política de autenticación y portal de autenticación.	cuando los usuarios envían nombres de usuario corporativos a sitios en una categoría restringida. Dado que este método busca una coincidencia entre la dirección IP de nombre de usuario de inicio de sesión asociado a la sesión y la tabla de asignación de dirección IP a nombre de usuario, se trata de un método eficaz para la detección de envíos de nombres de usuario corporativos, pero no detecta el envío de contraseñas corporativas. Si desea detectar el envío de nombres de usuario y contraseñas corporativas, debe utilizar el método de filtro de credenciales de dominio.
Filtro de credenciales de dominio	Agente de User-ID de Windows configurado con el elemento adicional del servicio de credenciales de User-ID - Y - Asignaciones de direcciones IP a nombres de usuario identificadas mediante la asignación de usuarios, GlobalProtect o la Política de autenticación y portal de autenticación.	El cortafuegos realiza la comprobación para determinar si el nombre de usuario y la contraseña que envía un usuario coinciden con el nombre de usuario y la contraseña corporativos del mismo usuario. Para ello, el cortafuegos debe ser capaz de encontrar una coincidencia entre los envíos de credenciales con nombres de usuario y contraseñas corporativos válidos, y comprobar si el nombre de usuario enviado se correlaciona con la dirección IP del nombre de usuario de inicio de sesión de la siguiente manera: • **Para detectar nombres de usuario y contraseñas corporativos:** el cortafuegos recupera una máscara de bits segura, denominada *filtro bloom*, de un agente de User-ID de Windows con el elemento adicional de credenciales de User-ID. Este servicio adicional analiza su directorio en busca de nombres de usuario y contraseñas hash, y los descompone en una máscara de bits segura (el filtro bloom) y la envía al agente de User-ID de Windows. El cortafuegos recupera el filtro boom del agente de User-ID de Windows en intervalos regulares. Si detecta que un usuario envía credenciales a una categoría restringida, descompone el filtro bloom, y busca un nombre de usuario y contraseña hash que coincida. El cortafuegos solo puede conectarse a un agente de User-ID de Windows que ejecuta el elemento adicional del servicio de credenciales de User-ID. • **Para comprobar que las credenciales pertenezcan al nombre de usuario de inicio de sesión:** el cortafuegos busca una asignación entre la dirección

Método para comprobar las credenciales enviadas	Requisitos de configuración de User-ID	¿Cómo detecta este método los nombres de usuario o las contraseñas corporativas que los usuarios envían a los sitios web?
		IP del nombre de usuario de inicio de sesión y el nombre de usuario detectado en su tabla de asignación de direcciones IP a nombres de usuario. Para obtener más información sobre el método de credenciales de dominio, consulte Configuración de la detección de credenciales con el agente de User-ID basado en Windows.

Configurar la detección de credenciales con el agente de User-ID de Windows

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

El filtro de credencial de dominio permite que el cortafuegos detecte contraseñas enviadas a las páginas web. Este método de detección de credenciales requiere que el agente de User-ID de Windows y el servicio de credencial de User-ID, un complemento del agente de User-ID, estén instalados en un controlador de *dominio de solo lectura (Read-Only Domain Controller, RODC).*

El método de detección Domain Credential Filter (Filtro de credenciales de dominio) solo se admite con el agente de User-ID de Windows. No puede configurarlo con el agente de User-ID integrado en PAN-OS.

Un RODC es un servidor Microsoft Windows que mantiene una copia de solo lectura de una base de datos de Active Directory que aloja un controlador de dominio. Cuando el controlador de dominio está ubicado en una sede corporativa; por ejemplo, los RODC pueden implementarse en ubicaciones de red remotas para proporcionar servicios de autenticación. La instalación del agente de ID de usuario en un RODC puede ser útil por algunos motivos: el acceso al directorio de controlador de dominio no es necesario para habilitar la detección de credenciales y usted puede admitir la detección de credenciales para un conjunto limitado u objetivo de usuarios. Debido a que el directorio que el RODC aloja es de solo lectura, el contenido del directorio permanece seguro en el controlador de dominio.

Como debe instalar el agente de User-ID de Windows en el RODC para garantizar la detección de credenciales, se recomienda implementar un agente distinto para este fin. No use el agente de User-ID que se instaló en el RODC para asignar direcciones IP a usuarios.

Después de instalar el agente de ID de usuario en un RODC, el servicio de credencial de ID de usuario se ejecuta en segundo plano y escanea el directorio para encontrar los hashes de nombres de usuario y contraseñas de miembros de grupo que se incluyen en la lista de la política de replicación de contraseña de RODC: puede definir quién desea que esté en la lista. El servicio de credencial de ID de usuario toma los hashes de nombre de usuario y contraseña recopilados y deconstruye los datos en un tipo de máscara de bits denominada *filtro de eclosión*. Los filtros de eclosión son estructuras de datos compactos que proporcionan un método seguro para comprobar si un elemento (un hash de nombre de usuario o contraseña) es miembro de un conjunto de elementos (los conjuntos de credenciales que aprobó para la replicación en el RODC). El servicio de credenciales de User-ID reenvía el filtro de eclosión al agente de User-ID de Windows; el cortafuegos recupera el último filtro de eclosión del agente de User-ID a intervalos periódicos y lo utiliza para detectar envíos de hashes de nombres de usuario y contraseñas. Según su configuración, el cortafuegos luego bloquea, alerta o permite los envíos de contraseña válidos a páginas web, o muestra una página de respuesta a los usuarios que les advierte los peligros de suplantación de identidad, pero les permite continuar con el envío.

A través de este proceso, el agente de ID de usuario no almacena ni expone hashes de contraseña, ni reenvía hashes de contraseña al cortafuegos. Una vez que los hashes de contraseña se deconstruyen en un filtro de eclosión, no hay manera de recuperarlos.

STEP 1 | Configure la asignación de usuarios mediante el agente de User-ID de Windows.

Para habilitar la detección de credenciales, debe instalar el agente de User-ID de Windows en un RODC. Consulte la Matriz de compatibilidad para ver una lista de servidores compatibles. Instale un agente de User-ID distinto para esto.

Elementos importantes para recordar al configurar la ID de usuario para habilitar la detección de filtro de credenciales de dominio:

- La eficacia de la detección de phishing de credenciales depende de la configuración de RODC. Asegúrese de revisar las prácticas recomendadas y recomendaciones para la Administración de RODC.
- Descargue las actualizaciones de software de ID de usuario:
  - Instalador de Windows de agente de ID de usuario: UaInstall-x.x.x-x.msi.
  - Instalador de Windows del servicio de credenciales del agente de ID de usuario: UaCredInstall64-x.x.x-x.msi.
- Instale el agente de ID de usuario y el servicio de credenciales del agente de usuario en un RODC usando una cuenta que tenga privilegios para leer Active Directory a través de LDAP (el agente de ID de usuario también necesita este privilegio).
  - El servicio de credenciales del agente de User-ID necesita permiso para iniciar sesión en la cuenta del sistema local. Para obtener más información, consulte Creación de una cuenta de servicio exclusiva para el agente de User-ID.
  - La cuenta de servicio debe formar parte del grupo de administradores locales del RODC.

STEP 2 | Habilite el agente de ID de usuario y el servicio de credencial de agente de usuario (que se ejecuta en segundo plano para escanear las credenciales permitidas) para que comparta información.

1. En el servidor RODC, inicie el agente de ID de usuario.
2. Seleccione **Setup (Configuración)** y modifique la sección Setup.
3. Seleccione la pestaña **Credentials (Credenciales)**. Esta pestaña se muestra únicamente si usted ya instaló el servicio de credenciales de agente de ID de usuario.
4. Seleccione **Import from User-ID Credential Agent (Importar del agente de credenciales de ID de usuario)**. Esto permite que el agente de ID de usuario importe el filtro de eclosión que el agente de credenciales de ID de usuario crea para representar a los usuarios y los hashes de contraseña correspondientes.
5. Haga clic en **OK (Aceptar)**, en **Save (Guardar)** para guardar los ajustes y en **Commit (Confirmar)**.

STEP 3 | En el directorio RODC, defina el grupo de usuarios para el cual desea admitir la detección de envío de credenciales.

- Confirme que los grupos que deben recibir el cumplimiento de envío de credenciales se añadan al grupo de replicación de contraseña RODC permitida.
- Verifique que ninguno de los grupos dentro del grupo de replicación de contraseña RODC permitida esté también en el grupo de replicación de contraseña no permitida. Los grupos enumerados en ambos no estarán sujetos al cumplimiento de la suplantación de identidad de credenciales.

STEP 4 | Continúe con la siguiente tarea.

Configure la prevención de phishing (suplantación de identidad) de credenciales en el cortafuegos.

Configuración de la prevención de suplantación de identidad de credenciales

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Una vez que haya decidido cuál método de detección de credenciales de usuarioconfigurar, siga estos pasos para evitar ataques exitosos de phishing de credenciales.

Antes de habilitar la prevención de suplantación de identidades de credenciales, compruebe que el Primary Username (Nombre de usuario principal) que configure en el cortafuegos utilice el atributo sAMAccountName. La prevención de suplantación de identidades de credenciales no admite atributos alternativos.

- Strata Cloud Manager
- PAN-OS y Panorama

Configuración de la prevención de suplantación de identidad de credenciales (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Configure el método de detección de credenciales de usuario que desea utilizar.

Revise métodos para verificar los envíos de credenciales corporativas para obtener detalles sobre cada método.

- Para la asignación de direcciones IP a usuarios, configure usuarios y grupos locales, la redistribución de identidades o la autenticación con Prisma Access.
- Para usar el filtro de credenciales de dominio, configure la redistribución de identidades y los usuarios y grupos locales o la Autenticación.
- Para usar Asignación de grupos, configure usuarios y grupos locales o Autenticación.

STEP 2 | Cree una regla de política de descifrado que descifre el tráfico que desea supervisar para ver si se envían credenciales de usuario.

STEP 3 | Crear o modificar un perfil de gestión de acceso a URL.

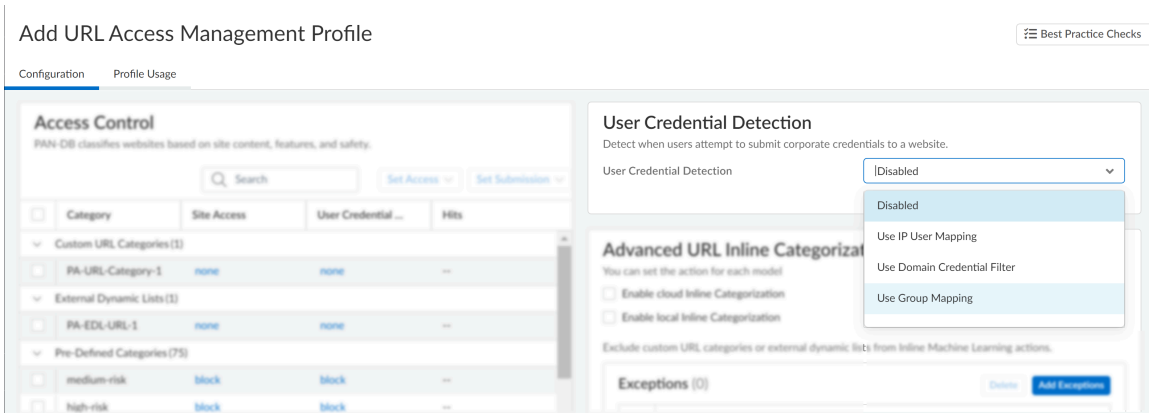
1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso de URL)**.
2. En Perfiles de gestión de acceso a URL, haga clic en **Add Profile (Añadir perfil)** o seleccione un perfil existente.

STEP 4 | Configure la configuración de detección de credenciales de usuario.

1. En Detección de credenciales de usuario, seleccione un método de **User Credential Detection (Detección de credenciales de usuario)**.
   - **Use IP User Mapping (Usar asignación de usuario IP)**: comprueba el envío de nombres de usuario corporativo válidos y verifica que el nombre de usuario que inició sesión esté asignado a la dirección IP de la sesión. Para esto, Prisma Access compara el nombre de usuario enviado y la dirección IP de origen de la sesión con su tabla de asignación de direcciones IP a usuarios.
   - **Use Domain Credential Filter (Usar filtro de credenciales de dominio)**: comprueba el envío de nombres de usuario y contraseñas válidas, y verifica que el nombre de usuario esté asignado a la dirección IP del usuario registrado.

- **Use Group Mapping (Usar asignación de grupo)**: comprueba el envío de nombres de usuario válidos en función de la tabla de asignación de usuario a grupo completada cuando asigna usuarios a grupos. Puede aplicar la detección de credenciales a cualquier parte del directorio o para grupos específicos que tengan acceso a sus aplicaciones más sensibles, como TI.

  Este método es propenso a falsos positivos en entornos que no tienen nombres de usuario estructurados de forma única. Por ello, solo debe usar este método para proteger sus cuentas de usuario más importantes.



2. Para la **Valid Username Detected Log Severity (Gravedad de log detectada en nombre de usuario válido)**, seleccione el nivel de gravedad que el cortafuegos registra en el log cuando detecta envíos de credenciales corporativas:
   - **high (alto)**
   - (por defecto) **medium (medio)**
   - **low (bajo)**

STEP 5 | Configure la acción realizada cuando el cortafuegos detecte envíos de credenciales corporativas.

1. En Control de acceso, seleccione una acción para **User Credential Submission (Envío de credenciales de usuario)** para cada categoría de URL con su **Site Access (Acceso al sitio)** configurado para permitir o alertar.

   Puede seleccionar entre las siguientes acciones:

   - (Recomendada) **alert (alertar)**: permite a los usuarios enviar credenciales a sitios web de la categoría URL determinada, pero genera un log de filtrado de URL cada vez que esto sucede.
   - (Predeterminada) **allow (permitir)**: permite que los usuarios envíen sus credenciales al sitio web.
   - (Recomendada) **block (bloquear)**: impide que los usuarios envíen credenciales a los sitios web de la categoría URL determinada. Cuando un usuario intenta enviar credenciales, el cortafuegos muestra la página de bloqueo antiphishing.
   - **continue (continuar)**: presenta la página de continuación antiphishing a los usuarios cuando intentan enviar credenciales. Los usuarios deben seleccionar Continuar en la página de respuesta para acceder al sitio web.

2. Seleccione **Save (Guardar)** el perfil.

STEP 6 | Aplique el perfil de gestión de acceso URL a sus reglas de la política de seguridad.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **Security Policy (Política de seguridad)**.
2. En Reglas de la política de seguridad, cree o seleccione una regla de la política de seguridad.
3. Seleccione **Actions (Acciones)** > **Profile Group (Grupo de perfiles)**y, a continuación, seleccione un grupo de perfiles de gestión de acceso a URL.
4. Seleccione **Save (Guardar)** la regla.

STEP 7 | Haga clic en **Push Config (Enviar configuración)**.

Configuración de la prevención de suplantación de identidad de credenciales (PAN-OS y Panorama)

STEP 1 | Habilitar User-ID.

Cada uno de los métodos para comprobar los envíos de credenciales corporativas exige una configuración de User-ID diferente:

- Asignación de grupos: detecta si un usuario está enviando un nombre de usuario corporativo válido y requiere que usted asigne usuarios a grupos.
- Asignación de usuarios de IP: detecta si un usuario está enviando un nombre de usuario corporativo válido y si el nombre de usuario coincide con el nombre de usuario de inicio de sesión; requiere que usted asigne direcciones IP a los usuarios.
- Filtro de credenciales de dominio: detecta si un usuario está enviando un nombre de usuario y una contraseña válidos, y si esas credenciales pertenecen al usuario que inició sesión.

requiere que configure la detección de credenciales con el agente de User-ID basado en Windows y asigne direcciones IP a los usuarios.

STEP 2 | Configure un perfil de filtrado de URL recomendado para garantizar protección contra las URL que se observó que alojan malware o contenido de exploits.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y **Add (Añadir)** para añadir o modificar un perfil de filtrado de URL.
2. Bloquee el acceso a todas las categorías URL peligrosas conocidas: malware, phishing, DNS dinámico, desconocidas, de comando y control, extremistas, de infracción de derechos de autor, de anonimización y anulación de proxy, de dominio recién registrado, grayware y estacionadas.

STEP 3 | Cree una regla de política de descifrado que descifre el tráfico que desea supervisar para los envíos de credenciales de usuario.

STEP 4 | Detecte envíos de credenciales corporativas a sitios web que se encuentran en categorías de URL permitidas.

Para proporcionar el mejor rendimiento, el cortafuegos no verifica los envíos de credenciales para sitios de confianza, incluso si habilita las verificaciones de las categorías de URL para estos sitios, para proporcionar el mejor rendimiento. Los sitios de confianza son sitios para los que Palo Alto Networks no ha observado ningún ataque malicioso o de phishing. Las actualizaciones para esta lista de sitios de confianza se realizan a través de actualizaciones de contenido de aplicaciones y amenazas.

1. Seleccione un perfil de filtrado de URL [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**] para modificar.
2. Seleccione **User Credential Detection (Detección de credenciales de usuario)** y elija uno de los métodos de detección de credenciales de usuario.

   Confirme que el formato del nombre de usuario principal es idéntico al formato del nombre de usuario que proporciona el origen de User-ID.

   - **Use IP User Mapping (Usar asignación de usuario IP):** comprueba el envío de nombres de usuario corporativo válidos y verifica que el nombre de usuario que inició sesión esté asignado a la dirección IP de la sesión. Para esto, el cortafuegos compara el nombre de usuario enviado y la dirección IP de origen de la sesión con su table de asignación de direcciones IP a usuarios. Para utilizar este método, configure cualquiera de los métodos de asignación de usuarios enumerados en Asignar direcciones IP a usuarios.
   - **Use Domain Credential Filter (Usar filtro de credenciales de dominio)**: comprueba el envío de nombres de usuario y contraseñas válidas, y verifica que el nombre de usuario esté asignado a la dirección IP del usuario registrado. Para obtener instrucciones sobre cómo configurar este método, consulte Configurar la detección de credenciales con el agente de User-ID basado en Windows.

- **Use Group Mapping (Usar asignación de grupo)**: comprueba el envío de nombres de usuario válidos en función de la tabla de asignación de usuario a grupo completada cuando configura el cortafuegos para la asignación de usuarios a grupos.

  Con la asignación de grupos, puede aplicar la detección de credenciales a cualquier parte del directorio o a grupos específicos que tienen acceso a sus aplicaciones más sensibles, como TI.

  Este método es propenso a falsos positivos en entornos que no poseen nombres de usuario estructurados de manera inequívoca. Por ello, solo debe usar este método para proteger sus cuentas de usuario más importantes.

3. Configure la **Valid Username Detected Log Severity (Gravedad del log detectado de nombre de usuario válido)** que el cortafuegos utilizará para la detección de logs de envío de credenciales corporativas. De manera predeterminada, el cortafuegos registra estos eventos como eventos de gravedad intermedia.

STEP 5 | Bloquee (o alerte) los envíos de credenciales a sitios permitidos.

1. Seleccione **Categories (Categorías)**.
2. Para cada categoría a la cual se permite el **Site Access (Acceso al sitio)**, seleccione cómo desea que se manejen los **User Credential Submissions (Envíos de credenciales de usuario)**:
   - **alert (alerta)**: permite que los usuarios envíen sus credenciales al sitio web, pero genera un log de filtrado de URL cada vez que un usuario envía credenciales a sitios de esta categoría de URL.
   - **allow (permitir)**: (predeterminado) permite que los usuarios envíen sus credenciales al sitio web.
   - **block (bloquear)**: impide que usuarios envíen credenciales al sitio web. Cuando un usuario intenta enviar credenciales, el cortafuegos muestra la página de bloqueo antiphishing, que impide el envío.
   - **Continue (Continuar)**: muestra la página de continuación antiphishing a los usuarios cuando intentan enviar credenciales. Los usuarios deben seleccionar Continue (Continuar) en la página de respuesta para continuar con el envío.
3. Seleccione **OK (Aceptar)** para guardar el perfil de filtro de URL.

STEP 6 | Aplique el perfil de filtrado de URL con los ajustes de detección de credenciales a sus reglas de la política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)** y **Add (Añadir)** o modifique una regla de la política de seguridad.
2. En la pestaña **Actions (Acciones)**, configure el **Profile Type (Tipo de perfil)** en **Profiles (Perfiles)**.
3. Seleccione el perfil **URL Filtering (Filtrado de URL)** nuevo o actualizado para adjuntarlo a la regla de la política de seguridad.
4. Seleccione **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 7 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 8 | Supervise los envíos de credenciales que el cortafuegos detecte.

*Seleccione **ACC** > **Hosts Visiting Malicious URLs (Hosts de visitas a URL malintencionadas)** para ver la cantidad de usuarios que visitaron sitios de malware y phishing.*

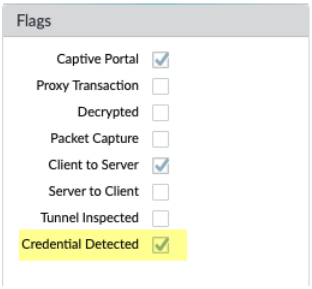
Seleccione **Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**.

La nueva columna **Credential Detected (Credencial detectada)** indica eventos en los que el cortafuegos detectó una solicitud post HTTP que incluía una credencial válida:

	CATEGORY	APPLICATION	ACTION	CREDENTIAL DETECTED
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes
	streaming-media		block-url	yes

(Para visualizar esta columna, pase el ratón sobre cualquier encabezado de columna y haga clic en la flecha para seleccionar las columnas que desea visualizar).

Los detalles de entrada del log también indican el envío de credenciales:



STEP 9 | Valide y solucione problemas de detección del envío de credenciales.

- Use el siguiente comando CLI para visualizar las estadísticas de detección de credenciales:

```
> show user credential-filter statistics
```

El resultado de este comando varía según el método configurado para que el cortafuegos detecte envíos de credenciales. Por ejemplo, si el método Domain Credential Filter (Filtro de

credenciales de dominio) está configurado en un perfil de filtrado de URL, se muestra una lista de agentes de User-ID que han reenviado un filtro de eclosión al cortafuegos, junto con la cantidad de credenciales incluidas en el filtro de eclosión.

- (Asignación de grupos únicamente) Utilice el siguiente comando CLI para ver información de asignación de grupos, incluido el número de perfiles de filtrado de URL con la detección de credenciales de asignación de grupos habilitada y los nombres de usuario de los miembros del grupo que intentaron enviar las credenciales a un sitio restringido.

  ```
  > show user group-mapping statistics
  ```

- (Filtro de credenciales de dominioMétodo únicamente) Utilice el siguiente comando de la CLI para ver todos los agentes de User-ID basados en Windows que envían asignaciones al cortafuegos:

  ```
  > show user user-id-agent state all
  ```

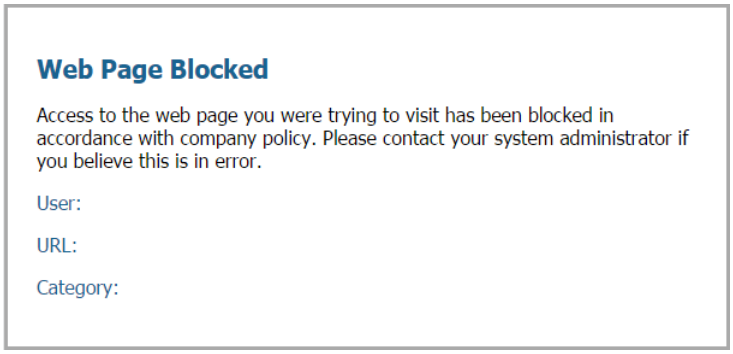
  El resultado del comando ahora muestra recuentos de filtros de eclosión que incluyen la cantidad de actualizaciones de filtro de eclosión que el cortafuegos ha recibido de cada agente, si alguna actualización de filtro de eclosión no se pudo procesar y cuántos segundos han pasado desde la última actualización de filtro de eclosión.

- (Filtrado de credenciales de dominio únicamente) El agente de User-ID basado en Windows muestra los mensajes de log que el filtro de eclosión (bloom filter, BF) de referencia envía al cortafuegos. En la interfaz del agente de User-ID, seleccione **Monitoring (Supervisión)** > **Logs**.

Páginas de respuesta de filtrado de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Las páginas de respuesta de filtrado de URL notifican a los usuarios cuando se ha restringido el acceso a una URL solicitada. El acceso puede estar restringido si un sitio pertenece a una categoría que se ha configurado con una acción de bloqueo, continuación o anulación, o si se han bloqueado los envíos de credenciales al sitio o la categoría. Si un usuario no tiene configuradas las configuraciones de búsqueda segura más estrictas para un motor de búsqueda y una regla de la política de seguridad impone una búsqueda segura, el acceso también estará restringido. Existen cinco páginas de respuesta predefinidas para dar cuenta de estos motivos. Algunas páginas de respuesta bloquean directamente el acceso, mientras que otras permiten el acceso condicional. Por ejemplo, si aparece la página Continuación y cancelación de filtrado de URL o la página Continuación antiphishing, los usuarios pueden hacer clic en Continuar para acceder al sitio (a menos que la Anulación de administrador de URL esté habilitada).



En general, las páginas de respuesta indican por qué no se puede acceder a la página y enumeran el usuario, la URL y la categoría de la URL. Sin embargo, puede personalizar el contenido y la apariencia de las páginas de respuesta. Por ejemplo, puede cambiar el mensaje de notificación, vincularlo a su política de uso aceptable o añadir la marca corporativa.

Es posible que observe variaciones en la apariencia de las páginas de respuesta en diferentes versiones de software PAN-OS. Sin embargo, la funcionalidad sigue siendo la misma.

Recuerde que puede personalizar las páginas de respuesta para satisfacer sus necesidades específicas.

Los navegadores no muestran páginas de respuesta si las Inspecciones de protocolo de enlace SSL/TLS están habilitadas.

- Páginas de respuesta de filtrado de URL predefinidas
- Objetos de página de respuesta de filtrado de URL
- Personalizar las páginas de respuesta de filtrado de URL

Páginas de respuesta de filtrado de URL predefinidas

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

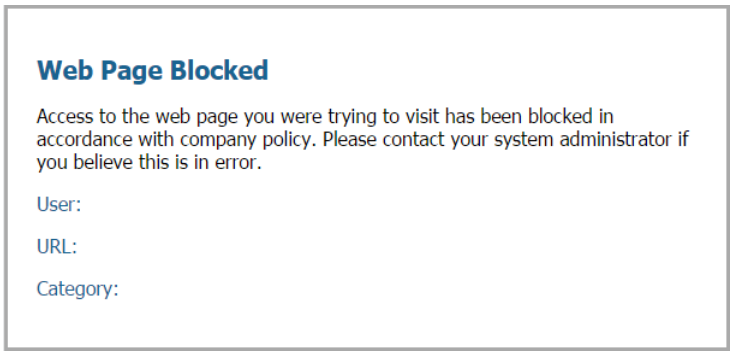
Las Páginas de respuesta de filtrado de URL se muestran en los navegadores web cuando se ha restringido el acceso a una URL solicitada. Cada página de respuesta explica por qué no se puede acceder a la página, y la mayoría de las páginas enumeran información sobre el usuario, la URL solicitada y la categoría de URL que desencadenó la acción de bloqueo.

Es posible que observe variaciones en la apariencia de las páginas de respuesta en diferentes versiones de software PAN-OS. Sin embargo, la funcionalidad sigue siendo la misma.

Recuerde que puede personalizar las páginas de respuesta para satisfacer sus necesidades específicas.

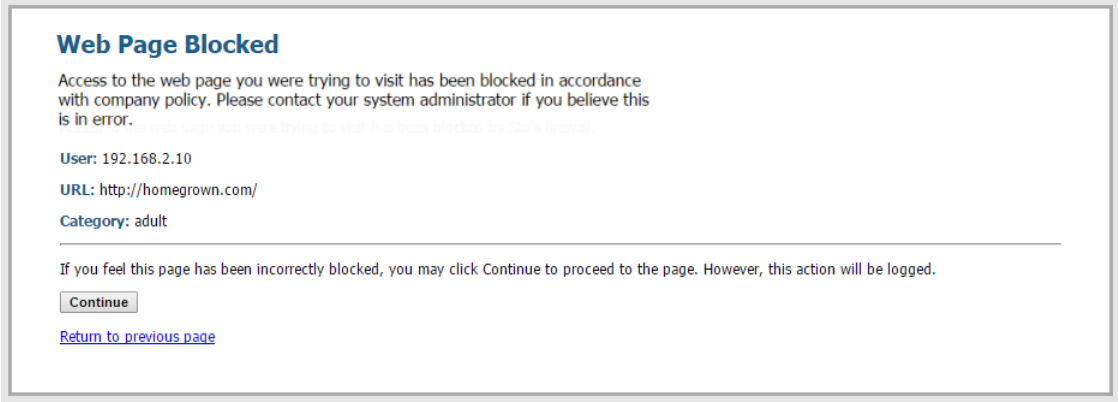
- **Filtrado de URL y página de bloqueo de coincidencia de categoría**

  Acceso bloqueado por un perfil de filtrado de URL o porque la categoría de URL está bloqueada por una regla de la política de seguridad.



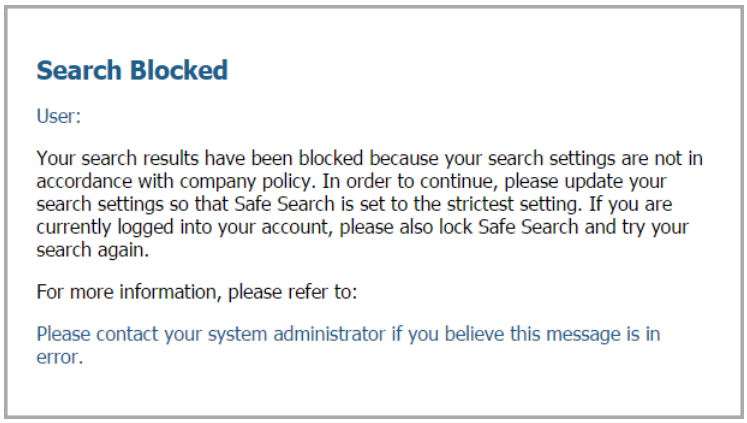
- **Página de continuación y cancelación de filtrado de URL**

Página con la política de bloqueo inicial que permite a los usuarios omitir el bloqueo al hacer clic en **Continue (Continuar)**. Con la cancelación de administración de URL habilitada, (Habilitación del acceso a determinados sitios mediante contraseña), después de hacer clic en **Continue (Continuar)**, el usuario debe proporcionar una contraseña para cancelar la política que bloquea la URL.



- **Página de bloque de búsqueda segura de filtrado de URL**

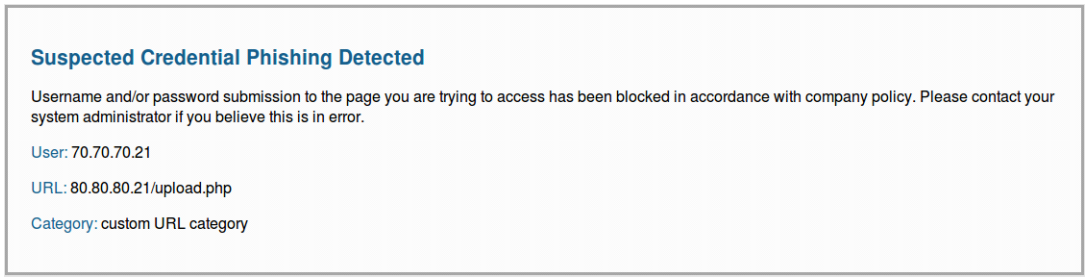
  Acceso bloqueado por una regla de la política de seguridad con un perfil de URL Filtering que tiene habilitada la opción Aplicación de búsquedas seguras (consulte Aplicación de búsquedas seguras). El usuario verá esta página si se realiza una búsqueda con Google, Bing, Yahoo o Yandex y la configuración de cuenta de su explorador o motor de búsqueda para la búsqueda segura no está establecida como estricta.



- **Página de bloqueo antiphishing**

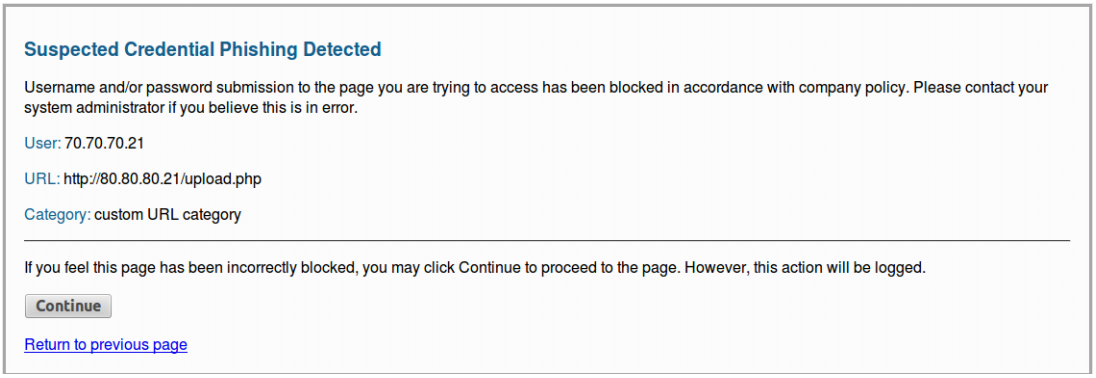
  Esta página se muestra a los usuarios cuando intentan introducir credenciales corporativas (nombres de usuario o contraseñas) en una página web, con una categoría para la cual se bloqueó la presentación de credenciales. El usuario puede seguir accediendo al sitio, pero sigue sin poder enviar credenciales corporativas válidas a formularios web asociados. Para controlar

los sitios a los que los usuarios pueden enviar credenciales corporativas, debe configurar el User-ID y habilitar la prevención de phishing de credenciales basado en la categoría de URL.



- **Página de continuación antiphishing**

  Esta página advierte a los usuarios sobre el envío de credenciales (nombres de usuario y contraseñas) a un sitio web. La advertencia a los usuarios contra la presentación de credenciales puede ayudar a disuadirlos de reutilizar credenciales corporativas y educarlos sobre posibles intentos de phishing. Deben seleccionar Continue (Continuar) para introducir las credenciales en el sitio. Para controlar los sitios a los que los usuarios pueden enviar credenciales corporativas, debe configurar el User-ID y habilitar la prevención de phishing de credenciales basado en la categoría de URL.



Objetos de página de respuesta de filtrado de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Utilice las variables y referencias descritas en las siguientes secciones para personalizar las páginas de respuesta de filtrado de URL. Las variables de la página de respuesta muestran información

diferente sobre las solicitudes de URL. Por ejemplo, el cortafuegos reemplaza la variable de `<category/>` en el código HTML para las páginas de respuesta con las categorías de URL de una URL solicitada. Las referencias de la página de respuesta le permiten añadir imágenes externas, sonidos, hojas de estilo y enlaces.

Variables de la página de respuesta

La siguiente tabla enumera las variables de la página de respuesta, y la información u objeto con el que el sistema sustituye cada variable durante un evento de bloqueo. Cada página de respuesta de filtrado de URL utiliza las siguientes variables de forma predeterminada: usuario, URL y categoría. Sin embargo, las páginas de respuesta son personalizables. Por ejemplo, puede modificar el orden de las variables o añadir mensajes diferentes para categorías de URL específicas.

Variable	Uso
<user/>	El cortafuegos sustituye la variable por el nombre de usuario (si está disponible mediante User-ID) o la dirección IP del usuario cuando se muestra la página de respuesta.
<url/>	El cortafuegos sustituye la variable por la dirección URL solicitada cuando se muestra la página de respuesta.
<category/>	El cortafuegos sustituye la variable por la categoría de filtrado de URL de la solicitud bloqueada.
<pan_form/>	Código HTML para mostrar el botón **Continue (Continuar)** en la página de continuación y cancelación de filtrado de URL.

Además, puede añadir código que active el cortafuegos para mostrar el uso de distintos mensajes según la categoría de URL a la que el usuario está intentando acceder. Por ejemplo, el siguiente fragmento de código de una página de respuesta especifica que se muestre el mensaje 1 si la categoría de URL es games, el mensaje 2 si la categoría es travel o el mensaje 3 si la categoría es kids:

```
var cat = "<category/>"; switch(cat) { case 'games':
 document.getElementById("warningText").innerHTML = "Message 1";
 break; case 'travel':
 document.getElementById("warningText").innerHTML = "Message 2";
 break; case 'kids': document.getElementById("warningText").innerHTML
 = "Message 3"; break; }
```

Referencias de página de respuesta

Solo se puede cargar una página HTML en cada sistema virtual para cada tipo de página de bloqueo. Sin embargo, otros recursos como las imágenes, los sonidos y las hojas de estilos en cascada (archivos CSS) se pueden cargar de otros servidores en el momento en el que se muestra la página de respuesta en el explorador. Todas las referencias deben incluir una dirección URL completa.

Tipo de referencia	Código HTML de ejemplo
Imagen	`<img src="http://virginiadot.org/images/Stop-Sign-gif.gif">`
Sonido	`<embed src="http://simplythebest.net/sounds/WAV/WAV_files/ movie_WAV_files/ do_not_go.wav" volume="100" hidden="true" autostart="true">`
Hoja de estilos	`<link href="http://example.com/style.css" rel="stylesheet" type="text/css" />`
Hiperenlace	`<a href="http://en.wikipedia.org/wiki/Acceptable_use_policy">Ver Política corporativa</a>`

Personalizar las páginas de respuesta de filtrado de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

De forma predeterminada, las páginas de respuesta de filtrado de URL explican por qué no se puede acceder a una URL solicitada y muestran la dirección IP del usuario, la URL solicitada y la categoría de URL. Puede personalizar las páginas de respuesta para satisfacer las necesidades de su empresa. Por ejemplo, puede cambiar el mensaje que se muestra a los usuarios, añadir marca corporativa o vincular a una política de uso aceptable.

Para personalizar una página, exportarla desde una plataforma y modificarla en un editor de texto. Puede realizar actualizaciones utilizando las referencias y variables de la página de respuesta proporcionadas. Las variables de la página de respuesta corresponden al usuario, URL y categoría específicos que se bloquearon. Las referencias de página de respuesta permiten el uso de imágenes, sonidos, hojas de estilo y enlaces.

La interfaz web de Panorama™ no admite la exportación de páginas de respuesta.

Las páginas de respuesta personalizadas más grandes que el tamaño máximo admitido no se descifran ni muestran a los usuarios. En PAN-OS 8.1.2 y versiones anteriores de PAN-OS 8.1, las páginas de respuesta personalizadas en un sitio descifrado no pueden superar los 8.191 bytes; el tamaño máximo es 17.999 bytes en PAN-OS 8.1.3 y versiones posteriores.

- Strata Cloud Manager
- PAN-OS y Panorama

Personalizar las páginas de respuesta del filtrado de URL (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Exporte las páginas de respuesta predeterminadas que desee personalizar.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y)Prisma Access** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)** > **Settings (Configuración)**.
2. En el panel Páginas de respuesta, haga clic en **Export HTML Template (Exportar plantilla HTML)** para cada página de respuesta que desee editar.
3. Guarde los archivos en su sistema.

STEP 2 | Editar una página de respuesta exportada.

1. Con el editor de texto de HTML que prefiera, edite la página:
   - Para mostrar información personalizada sobre el usuario, la URL o la categoría específicos que fueron bloqueados, añada una o más variables de página de respuesta.
   - Para incluir imágenes, sonidos, hojas de estilo o enlaces personalizados, incluya una o más referencias de páginas de respuesta.
2. Guarde la imagen editada con un nuevo nombre de archivo.

   *Asegúrese de que la página conserva su codificación UTF-8. Por ejemplo, en el Bloc de notas seleccionaría **UTF-8** del menú desplegable **Encoding (Codificación)** en el cuadro de diálogo Guardar como.*

STEP 3 | Importe la página de respuesta personalizada.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y)Prisma Access** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)** > **Settings (Configuración)**.
2. En el panel Páginas de respuesta, haga clic en el tipo de página de respuesta que personalizó. Aparece un cuadro de diálogo de selección de archivos.

   Por ejemplo, si personalizó la página de bloqueo de gestión de acceso URL, deberá hacer clic en **Página de bloqueo de gestión de acceso URL**.

3. Haga clic en **Choose File (Seleccionar archivo)** y luego seleccione el archivo que ha personalizado.
4. Haga clic en **Save (Guardar)**.

STEP 4 | Haga clic en **Push Config (Enviar configuración)**.

STEP 5 | Verifique que se muestre la página de respuesta personalizada.

Desde un navegador web, visite una URL que activará la página de respuesta. Por ejemplo, para verificar una página de bloqueo de gestión de acceso URL personalizada, visite una URL bloqueada por sus reglas de la política de seguridad.

El cortafuegos utiliza los siguientes puertos para mostrar las páginas de respuesta de gestión de acceso URL:

- **HTTP**: 6080
- **Default TLS with firewall certificate (TLS predeterminado con certificado de cortafuegos)**: 6081
- **Custom SSL/TLS profile (Perfil SSL/TLS personalizado)**: 6082

Personalizar las páginas de respuesta de filtrado de URL (PAN-OS y Panorama)

STEP 1 | Exporte las páginas de respuesta predefinidas que desee personalizar.

La interfaz web de Panorama no admite la exportación de páginas de respuesta. Puede exportar páginas de respuesta directamente desde la interfaz web de un cortafuegos específico o utilizar el menú desplegable de Contexto en la interfaz web de Panorama para cambiar rápidamente a la interfaz web de un cortafuegos gestionado.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el **Type (Tipo)** de página de respuesta que desea editar. Aparece un cuadro de diálogo para la página de respuesta específica.
3. Seleccione **Predefined (Predefinido)** y luego seleccione **Export (Exportar)**.
4. Ahora debe **Close (Cerrar)** el diálogo.

   (Opcional) Repita los pasos dos a cuatro para páginas de respuesta adicionales.
5. Guarde los archivos en su sistema.

STEP 2 | Personalice una página de respuesta HTML exportada.

1. Abra el archivo en un editor de texto preferido.
   - Para mostrar información personalizada sobre un usuario específico, una URL solicitada o una categoría de URL bloqueada, utilice las variables de la página de respuesta.
   - Para integrar imágenes, sonidos, hojas de estilo o enlaces personalizados, utilice referencias de página de respuesta.
2. Guarde el archivo editado con un nuevo nombre.

   *Asegúrese de que la página conserva su codificación UTF-8. Por ejemplo, en el Bloc de notas, debe seleccionar **UTF-8** en la lista desplegable **Encoding (Codificación)** del cuadro de diálogo Guardar como.*

STEP 3 | Importe la página de respuesta personalizada.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Seleccione el **Type (Tipo)** de página de respuesta que editó. Aparece un cuadro de diálogo para la página de respuesta específica.
3. Seleccione **Predefined (Predefinido)** y luego seleccione **Import (Importar)**. Aparece un cuadro de diálogo Importar archivo.

   Para **Import File (Importar archivo)**, seleccione **Browse (Examinar)** la página de respuesta editada.
4. (Opcional) Para **Destination (Destino)**, seleccione el sistema virtual que va a utilizar la página de respuesta o seleccione **shared (compartido)** para que esté disponible para todos los sistemas virtuales.
5. Haga clic en **OK (Aceptar)** y luego en **Close (Cerrar)** para cerrar el cuadro de diálogo.

STEP 4 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 5 | Pruebe la página de respuesta personalizada.

Desde un navegador web, visite una URL que active la página de respuesta particular. Por ejemplo, para verificar una página de respuesta de filtrado de URL y coincidencia de categoría, visite una URL bloqueada en una regla de la política de seguridad. Verifique que sus cambios aparezcan.

El cortafuegos utiliza los siguientes puertos para mostrar las páginas de respuesta de filtrado de URL:

- **HTTP**: 6080
- **Default TLS with firewall certificate (TLS predeterminado con certificado de cortafuegos)**: 6081
- **Custom SSL/TLS profile (Perfil SSL/TLS personalizado)**: 6082

Aplicación de búsquedas seguras

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.* • SafeSearch transparente requiere una licencia de Prisma Access que ejecuta una versión mínima de 4.1.

Muchos motores de búsqueda ofrecen una configuración de búsqueda segura que le permite filtrar contenido para adultos de los resultados de búsqueda. Las configuraciones de filtro generalmente incluyen `Moderado`, `Estrictoy` `Desactivado`. Puede utilizar la configuración moderada para filtrar solo imágenes y vídeos para adultos o la configuración estricta, que además filtra el texto explícito. Los centros educativos, los lugares de trabajo, los niños y los adultos se benefician de esta función de búsqueda segura. Sin embargo, permitir que los usuarios de su red configuren los ajustes de búsqueda segura no siempre proporciona la protección que necesita.

Para proteger su red de contenido para adultos, puede aplicar la configuración de búsqueda segura más estricta para todos los usuarios finales; independientemente de su configuración individual actual. La configuración de búsqueda segura más estricta proporciona la experiencia de navegación más segura. Primero, seleccione la opción **Safe Search Enforcement (Aplicación de búsquedas seguras)** en un perfil de filtrado de URL. Luego, aplique el perfil a cualquier regla de la política de seguridad que permita el tráfico de clientes en la zona de confianza a Internet.

Ni los proveedores de motores de búsqueda ni Palo Alto Networks pueden garantizar la precisión total del filtrado. Los motores de búsqueda clasifican los sitios web como seguros o no seguros. Como tal, un sitio web clasificado como seguro puede contener contenido explícito. Palo Alto Networks aplica un filtrado basado únicamente en los mecanismos de filtrado del motor de búsqueda.

El cortafuegos puede aplicar las siguientes opciones cuando los usuarios buscan con Bing, Yahoo, Yandex o YouTube y no han establecido la configuración de búsqueda segura para estos motores en el nivel más estricto:

- Bloquear resultados de búsqueda cuando la búsqueda segura estricta no está habilitada (predeterminado): el cortafuegos impide que los usuarios finales vean los resultados de búsqueda hasta que configuren su búsqueda segura en la opción más estricta disponible. En este escenario, el navegador muestra la página de bloqueo de búsqueda segura de filtrado de URL. Esta página de respuesta permite a los usuarios finales saber por qué se bloquearon

sus resultados de búsqueda e incluye un enlace a la configuración de búsqueda del motor de búsqueda utilizado para dicha búsqueda.

> *Palo Alto Networks ya no puede detectar si Google SafeSearch está habilitado debido a cambios en la implementación de búsqueda segura de Google. Como resultado, el método de bloqueo no funciona para las búsquedas de Google. En su lugar, puede configurar Google SafeSearch utilizando los métodos descritos en* Configuración de búsqueda segura para proveedores de búsqueda.

- Forzar búsqueda segura estricta (compatible únicamente con los motores de búsqueda Yahoo y Bing): el cortafuegos aplica de forma automática y transparente las configuraciones de búsqueda segura más estrictas. En concreto, el cortafuegos redirige las consultas de búsqueda a las URL que devuelven resultados de búsqueda estrictamente filtrados y cambia la preferencia de búsqueda segura para el motor de búsqueda utilizado. Para habilitar esta funcionalidad, sustituya el texto de la página de bloqueo de búsqueda segura del filtrado de URL con el texto especificado en el procedimiento. El texto de sustitución incluye código JavaScript, que reescribe las URL de las consultas de búsqueda con el parámetro de búsqueda segura estricto para el motor de búsqueda utilizado para la búsqueda.

  > *El navegador no muestra la página de bloqueo de búsqueda segura del filtrado de URL cuando utiliza este método.*

- SafeSearch transparente (Solo implementaciones de Prisma Access): en los casos en los que no se puede descifrar el tráfico (por ejemplo, en una tienda que proporciona acceso a Internet para invitados) y desea evitar que los usuarios con dispositivos no gestionados, incluidos los dispositivos de visualización, busquen material restringido, inapropiado u ofensivo; puede usar SafeSearch transparente en Prisma Access, que resuelve las consultas del motor de búsqueda de los usuarios móviles al portal SafeSearch del motor de búsqueda mediante la realización de una asignación de FQDN a IP.

Comience a implementar la búsqueda segura revisando la configuración de búsqueda segura de cada motor de búsqueda compatible. Luego, decida qué método de aplicación es mejor para su contexto.

- Configuración de búsqueda segura para proveedores de búsqueda
- Bloquear los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada
- Forzar búsqueda segura estricta
- Usar SafeSearch transparente en Prisma Access

Configuración de búsqueda segura para proveedores de búsqueda

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	• *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

La configuración de búsqueda segura varía según el proveedor de búsqueda; revise las siguientes configuraciones para obtener más información.

Proveedor de búsquedas	Descripción de la configuración de búsqueda segura
Google/YouTube	Permiten la búsqueda segura en equipos individuales o en toda la red mediante la dirección IP virtual de búsqueda segura de Google: **Aplicación forzada de búsquedas seguras en Google en equipos individuales:** En la sección de ajustes de búsqueda de Google, la opción **Filter explicit results (Filtrar resultados explícitos)** habilita la función de búsqueda segura. Una vez habilitada, la configuración se almacena en una cookie del explorador como FF= y se pasa al servidor cada vez que el usuario realiza una búsqueda en Google. La anexión de **`safe=active`** a una dirección URL de consulta de búsqueda de Google también habilita la configuración de búsqueda segura más estricta. **Aplicación forzada de búsquedas seguras en Google y YouTube mediante una dirección IP virtual** Google proporciona servidores que bloquean SafeSearch (forcesafesearch.google.com) en cada búsqueda de Google y YouTube. Si añade una entrada DNS para **`www.google.com`** y **`www.youtube.com`** (y otros subdominios correspondientes a países de Google y YouTube) que incluya un registro CNAME que apunte a **`forcesafesearch.google.com`** para la configuración de su servidor DNS, puede garantizar que todos los usuarios de su red usen la configuración de búsqueda segura estricta cada vez que realicen una búsqueda en Google o YouTube. Sin embargo, debe tener en cuenta que esa solución no es compatible con la aplicación forzada de búsquedas seguras en el cortafuegos. Así, si está usando esta opción para forzar las búsquedas seguras en Google, lo mejor es bloquear el acceso a otros motores de búsqueda del cortafuegos creando categorías de URL personalizadas y añadiéndolas a la lista de bloqueados en el perfil de filtrado de URL.

Proveedor de búsquedas	Descripción de la configuración de búsqueda segura
	 • *PAN-OS admite la aplicación de búsquedas seguras para YouTube mediante la inserción de encabezados HTTP. Actualmente, la inserción de encabezados HTTP no es compatible con HTTP/2. Para hacer cumplir la búsqueda segura de YouTube, la Inspección de App-ID y HTTP/2, cambie las versiones de las conexiones HTTP/2 a HTTP/1.1 utilizando la función **Strip ALPN (Eliminar ALPN)** en el perfil de descifrado adecuado.* • *Si planifica utilizar la solución de bloqueo SafeSearch de Google, considere la posibilidad de configurar un proxy DNS [**Network (Red)** > **DNS Proxy (Proxy DNS)**] y establecer el origen de herencia como la interfaz de Capa 3 en la que el cortafuegos recibe la configuración de DNS del proveedor de servicios mediante DHCP. Debe configurar el proxy DNS con **Entradas estáticas** para www.google.com y www.youtube.com mediante la dirección IP local para el servidor de forcesafesearch.google.com.*
Yahoo	Permite la búsqueda segura solamente en equipos individuales. Las preferencias de búsqueda de Yahoo incluyen tres opciones de SafeSearch: **Estricta**, **Moderada** o **Desactivada**. Una vez habilitada, la configuración se almacena en una cookie del explorador como `vm=` y se pasa al servidor cada vez que el usuario realiza una búsqueda en Yahoo.

Proveedor de búsquedas	Descripción de la configuración de búsqueda segura
	La anexión de `vm=r` a una dirección URL de consulta de búsqueda de Yahoo también habilita la configuración de búsqueda segura más estricta. *Cuando se realiza una búsqueda en Yahoo Japan (**`yahoo.co.jp`**) tras iniciar sesión con una cuenta de Yahoo, los usuarios finales deben habilitar la opción de bloqueo en **SafeSearch Lock (Bloquear)**.*
Bing	Ofrece la búsqueda segura en equipos individuales. La configuración de Bing incluye tres opciones de SafeSearch: **Estricta**, **Moderada** o **Desactivada**. Una vez habilitada, la configuración se almacena en una cookie del explorador como `adtl=` y se pasa al servidor cada vez que el usuario realiza una búsqueda en Bing. La anexión de **`adlt=strict`** a una dirección URL de consulta de búsqueda de Bing también habilita la configuración de búsqueda segura más estricta. El motor de búsqueda SSL de Bing no fuerza los parámetros de URL de búsqueda segura y, por lo tanto, debe considerar la posibilidad de bloquear Bing en SSL para la aplicación forzada de búsquedas seguras completa.

Bloquear los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Si habilita la aplicación de búsqueda segura, el comportamiento predeterminado del cortafuegos es bloquear los resultados de búsqueda para los usuarios finales que buscan en los motores

de búsqueda de Bing, Yahoo, Yandex o Youtube, hasta que establezcan su configuración de búsqueda segura en la opción más estricta disponible. Por defecto, la página de bloqueo de búsqueda segura de filtrado de URL se muestra en su navegador. La página de bloqueo predefinida proporciona un enlace a la configuración de búsqueda para el motor de búsqueda utilizado, de modo que los usuarios pueden ajustar la configuración de búsqueda segura. Puede personalizar la página de bloqueo de búsqueda segura para satisfacer las necesidades específicas de su organización.

Si tiene previsto usar este método para forzar la aplicación de búsqueda segura, debe comunicar la política a sus usuarios finales antes de implementarla. Si prefiere redirigir automáticamente las URL de las consultas de búsqueda de los usuarios finales a versiones de búsqueda segura estrictas, habilite la búsqueda segura estricta de forma transparente.

Palo Alto Networks ya no puede detectar si Google SafeSearch está activado debido a cambios en la implementación de Google. Como resultado, el cortafuegos no puede imponer una búsqueda segura utilizando este método. Aun así, puede forzar la aplicación de la búsqueda segura de forma transparente. Sin embargo, no podemos garantizar que Google filtrará imágenes y contenido explícito.

- Strata Cloud Manager
- PAN-OS y Panorama

Bloquear los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Habilite la aplicación de búsquedas seguras en un perfil de gestión de acceso URL.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En Perfiles de gestión de acceso URL, seleccione un perfil existente o **Add Profile (Añadir perfil)** para crear uno nuevo. Aparecen las opciones de configuración.
3. En **Settings (Configuración)**, seleccione **Safe Search Enforcement (Aplicación de búsquedas seguras)**.
4. Elija **Save (Guardar)** el perfil.

STEP 2 | (Opcional) Restrinja los motores de búsqueda a los que pueden acceder los usuarios finales.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En **Access Control (Control de acceso)**, seleccione **Search (Buscar)** ( ) para la categoría **search-engines (motores de búsqueda)**.
3. Establezca el acceso al sitio para la categoría **search-engines (motores de búsqueda)** en **block (bloquear)**.

   En un paso posterior, creará una categoría de URL personalizada (Tipo de lista de URL) con los motores de búsqueda que desea permitir.

4. Elija **Save (Guardar)** el perfil.

STEP 3 | Aplique el perfil de gestión de acceso URL a las reglas de la política de seguridad que permiten el tráfico de los clientes de la zona de confianza a Internet.

Para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad), añádalo al `grupo de perfiles` y haga referencia al grupo de perfiles en una regla de la política de seguridad.

STEP 4 | Cree una categoría de URL personalizada para los motores de búsqueda compatibles.

En el siguiente paso, configurará el cortafuegos para descifrar el tráfico a esta categoría personalizada.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En **Access Control (Control de acceso)**, para categorías de URL personalizadas, **Add Category (Añadir categoría)**.
3. Introduzca un nombre en **Name (Nombre)** para la categoría, como **`SearchEngineDecryption`**.
4. Para el **Type (Tipo)** de la categoría de URL personalizada, seleccione **URL List (Lista de URL)**.
5. En **Items (Elementos)**, seleccione **Add (Añadir)** las siguientes entradas a la lista de URL:
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. Seleccione **Save (Guardar)** la categoría personalizada.
7. Configure el acceso al sitio para la nueva categoría de URL personalizada.
   1. En Perfiles de gestión de acceso URL, seleccione el perfil que configuró anteriormente.
   2. En Control de acceso, seleccione la nueva categoría de URL personalizada. Esta aparece en la sección Categorías de URL personalizadas, encima de Listas de URL dinámicas externas y Categorías predefinidas.
   3. Establezca **Site Access (Acceso al sitio)** en **allow (permitir)**.
   4. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 5 | Configure el descifrado del proxy SSL de reenvío.

Dado que la mayoría de los motores de búsqueda cifran los resultados de búsqueda, debe habilitar el descifrado del proxy SSL de reenvío para que el cortafuegos pueda inspeccionar el tráfico de búsqueda y detectar la configuración de búsqueda segura.

En **Services and URLs (Servicios y URL)** de la regla de política de descifrado, haga clic en **Add URL Categories (Añadir categorías de URL)**. A continuación, seleccione la categoría de URL personalizada que creó anteriormente. Las nuevas categorías personalizadas se encuentran en la parte superior de la lista.

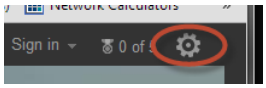
Debe **Save (Guardar)** la regla de la política de descifrado.

STEP 6 | Seleccione **Push Config (Enviar configuración)** para activar los cambios.

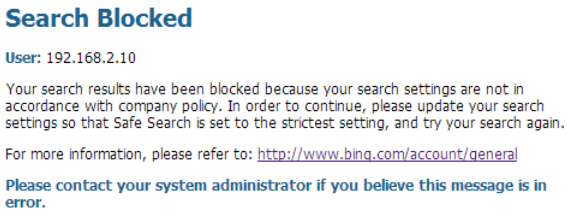
STEP 7 | Compruebe la configuración de la aplicación de búsquedas seguras.

Este paso de verificación solo funciona si usa bloquear páginas para la aplicación de la búsqueda segura. Hay un paso de verificación alternativo si habilita la búsqueda segura de forma transparente.

1. Desde un equipo detrás del cortafuegos, deshabilite la configuración de búsqueda estricta para un proveedor de búsqueda compatible. Por ejemplo, en bing.com, haga clic en el icono de **preferencias** en la barra de menús de Bing.



2. Establezca la opción **SafeSearch (Búsqueda segura)** en **Moderate (Moderada)** o **Off (Desactivada)** y haga clic en **Save (Guardar)**.
3. Realice una búsqueda en Bing (o una búsqueda con otro proveedor) para ver si se muestra la página de bloqueo de búsqueda segura de Gestión de acceso URL en lugar de los resultados de la búsqueda:



4. Utilice el vínculo de la página de bloqueo para actualizar la configuración de búsqueda segura a la configuración más estricta (**Strict (Estricta)** en el caso de Bing) y, a continuación, haga clic en **Save (Guardar)**.
5. Vuelva a realizar una búsqueda en Bing y compruebe si se muestran los resultados de la búsqueda filtrada en lugar de la página de bloqueo.

Bloquear los resultados de búsqueda cuando la búsqueda segura estricta no está habilitada (PAN-OS y Panorama)

STEP 1 | Habilite la aplicación de búsquedas seguras en un perfil de filtrado de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**.
2. Seleccione un perfil existente para modificarlo o duplique el perfil predeterminado para crear un nuevo perfil.
3. En la pestaña **URL Filtering Settings (Configuración de URL Filtering)**, seleccione **Safe Search Enforcement (Aplicación de búsquedas seguras)**.

STEP 2 | (Opcional) Restrinja los motores de búsqueda a los que pueden acceder los usuarios finales en el mismo perfil de filtrado de URL.

1. En la pestaña **Categories (Categorías)**, **Search (Busque)** ( ) la categoría **search-engines (motores de búsqueda)**
2. Establezca el acceso al sitio para la categoría **search-engines (motores de búsqueda)** en **block (bloquear)**.

   En un paso posterior, creará una categoría de URL personalizada (Tipo de lista de URL) con los motores de búsqueda que desea permitir.
3. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 3 | Aplique el perfil de URL Filtering a las reglas de la política de seguridad que permiten el tráfico de los clientes de la zona de confianza a Internet.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**. A continuación, haga clic en la regla a la que desea aplicar el perfil de URL Filtering.
2. En la pestaña **Actions (Acciones)**, busque Configuración de perfil. Para **Profile Type (Tipo de perfil)**, seleccione **Profiles (Perfiles)**. Aparece una lista de perfiles.
3. Para el perfil **URL Filtering (Filtrado de URL)**, seleccione el perfil que creó anteriormente.
4. Haga clic en **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 4 | Cree una categoría de URL personalizada para los motores de búsqueda compatibles.

En el siguiente paso, especificará que desea descifrar el tráfico a los sitios de la categoría personalizada.

1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría personalizada.
2. Introduzca un nombre en **Name (Nombre)** para la categoría, como **`SearchEngineDecryption`**.
3. Seleccione **Add (Añadir)** para añadir las siguientes entradas a la lista **Sites (Sitios)**:
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. Haga clic en **OK (Aceptar)** para guardar la categoría personalizada.
5. Configure el acceso al sitio para la nueva categoría de URL personalizada.
   1. Vaya a **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)** y seleccione el perfil de filtrado de URL que configuró anteriormente.
   2. En la pestaña **Category (Categoría)**, seleccione la nueva categoría de URL personalizada. Esta aparece en la sección Categorías de URL personalizadas, encima de Listas de URL dinámicas externas y Categorías predefinidas.
   3. Establezca **Site Access (Acceso al sitio)** en **allow (permitir)**.
   4. Haga clic en **OK (Aceptar)** para guardar los cambios.

STEP 5 | Configure el descifrado del proxy SSL de reenvío.

Dado que la mayoría de los motores de búsqueda cifran los resultados de búsqueda, debe habilitar el descifrado del proxy SSL de reenvío para que el cortafuegos pueda inspeccionar el tráfico de búsqueda y detectar la configuración de búsqueda segura.

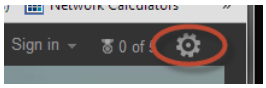
En la pestaña **Service/URL Category (Categoría de servicio/URL)** de la regla de política de descifrado, seleccione **Add (Añadir)** la categoría de URL personalizada que creó anteriormente. Después, haga clic en **OK (Aceptar)**.

STEP 6 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

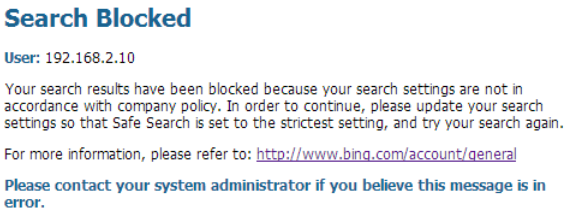
STEP 7 | Compruebe la configuración de la aplicación de búsquedas seguras.

Este paso de verificación solo funciona si usa bloquear páginas para la aplicación de la búsqueda segura. Hay un paso de verificación alternativo si habilita la búsqueda segura de forma transparente.

1. Desde un equipo detrás del cortafuegos, deshabilite la configuración de búsqueda estricta para un proveedor de búsqueda compatible. Por ejemplo, en bing.com, haga clic en el icono de **preferencias** en la barra de menús de Bing.



2. Establezca la opción **SafeSearch (Búsqueda segura)** en **Moderate (Moderada)** o **Off (Desactivada)** y haga clic en **Save (Guardar)**.
3. Realice una búsqueda en Bing (o una búsqueda con otro proveedor) para ver si se muestra la página Bloqueo de búsqueda segura de filtrado de URL en lugar de los resultados de la búsqueda:



4. Utilice el vínculo de la página de bloqueo para actualizar la configuración de búsqueda segura a la configuración más estricta (**Strict (Estricta)** en el caso de Bing) y, a continuación, haga clic en **Save (Guardar)**.
5. Vuelva a realizar una búsqueda en Bing y compruebe si se muestran los resultados de la búsqueda filtrada en lugar de la página de bloqueo.

Forzar búsqueda segura estricta

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama)	☐ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:***

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	• *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Puede proporcionar una experiencia de búsqueda segura y fluida para los usuarios finales de Bing y Yahoo al habilitar de forma transparente una búsqueda segura estricta. En lugar de bloquear los resultados de búsqueda cuando los usuarios finales buscan sin haber habilitado la búsqueda segura estricta, el cortafuegos activa automáticamente la búsqueda segura estricta y devuelve solo resultados de búsqueda estrictamente filtrados. Las escuelas y bibliotecas, por ejemplo, pueden beneficiarse de una aplicación automática que garantice una experiencia de aprendizaje coherente.

Para activar la aplicación de búsquedas seguras transparente, deberá habilitar la Aplicación de búsquedas seguras en un perfil de filtrado de URL y reemplazar el texto en el archivo de la página de bloqueo de búsqueda segura de filtrado de URL con el texto proporcionado en el siguiente procedimiento. El texto de reemplazo contiene JavaScript que añade URL de consultas de búsqueda con parámetros de búsqueda seguros estrictos para el motor de búsqueda utilizado para buscar.

La página de bloqueo de búsqueda segura de filtrado de URL no se muestra en el navegador.

Después de completar estos pasos, el cortafuegos ejecuta JavaScript cada vez que un usuario final realiza una búsqueda. Por ejemplo, supongamos que la preferencia de SafeSearch de Bing de un estudiante está `desactivada` cuando investiga un concepto que probablemente arroje resultados inapropiados. Al detectar la preferencia de búsqueda segura, el cortafuegos añade `&adlt=strict` a la URL de la consulta de búsqueda. Luego, el motor de búsqueda muestra resultados apropiados y la preferencia de SafeSearch cambia a `Estricta`.

- Strata Cloud Manager
- PAN-OS y Panorama

Forzar búsqueda segura estricta (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | Habilite la aplicación de búsquedas seguras en un perfil de gestión de acceso URL.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En Perfiles de gestión de acceso URL, seleccione un perfil existente o **Add Profile (Añadir perfil)** para crear uno nuevo. Aparecen las opciones de configuración.

3. En **Settings (Configuración)**, seleccione **Safe Search Enforcement (Aplicación de búsquedas seguras)**.
4. Seleccione **Save (Guardar)** el perfil.

STEP 2 | (Opcional) Restrinja los motores de búsqueda a los que pueden acceder los usuarios finales.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En **Access Control (Control de acceso)**, seleccione **Search (Buscar)** ( ) para la categoría **search-engines (motores de búsqueda)**.
3. Establezca el acceso al sitio para la categoría **search-engines (motores de búsqueda)** en **block (bloquear)**.

   En un paso posterior, creará una categoría de URL personalizada (Tipo de lista de URL) con los motores de búsqueda que desea permitir.
4. Seleccione **Save (Guardar)** el perfil.

STEP 3 | Aplique el perfil de gestión de acceso URL a las reglas de la política de seguridad que permiten el tráfico de los clientes de la zona de confianza a Internet.

Para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad), añádalo al `grupo de perfiles` y haga referencia al grupo de perfiles en una regla de la política de seguridad.

STEP 4 | Edite la página de bloqueo de búsqueda segura de la Gestión de acceso URL, reemplazando el código existente con JavaScript para reescribir las URL de las consultas de búsqueda.

1. Seleccione **Administrar** > **configuración** > **Servicios de seguridad** > **URL Administración de acceso** > **Páginas de respuesta**.
2. **Export HTML Template (Exportar plantilla HTML)** para la página de bloqueo de la gestión de acceso URL.
3. Utilice un editor HTML y sustituya todo el texto de la página de bloqueo existente con el siguiente texto. Luego, guarde el archivo.

```
<html> <head> <title>Búsqueda bloqueada</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>Búsqueda bloqueada</h1> <p> <b>Usuario:</b> <user/>
 </p> <p>Los resultados de búsqueda se han bloqueado porque
 la configuración de búsqueda no se ajusta a la política
 de la empresa. Para continuar, actualice la configuración
 de búsqueda para que Búsqueda segura se establezca en la
 configuración más estricta. Si actualmente ha iniciado
 sesión en su cuenta, bloquee también Búsqueda segura e
 intente su búsqueda nuevamente.</p> <p> Para obtener más
 información, consulte: <a href="<ssurl/>"> <ssurl/> </a> </p>
 <p id="java_off"> Habilite JavaScript en su navegador.<br></
```



```
p> <p><b>Póngase en contacto con el administrador del
 sistema si cree que este mensaje es un error.</b></p> </
div> </body> <script> Tome la URL que está en el navegador.
 var s_u = location.href; bing // Coincide con las barras
 diagonales al principio, cualquier cosa, luego ".bing."
 luego cualquier cosa seguida de una barra diagonal no
 expansiva. Hopefully the first forward slash. var b_a
 = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a) { s_u
 = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; } //
yahoo // Matches the forward slashes in the beginning,
 anything, then ".yahoo."" then anything followed by
 a non greedy slash. Esperemos que la primera barra
 hacia adelante. var y_a = /^.*\/\/(.+\.yahoo\..
+?)\//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

STEP 5 | Importe la página de bloqueo de búsqueda segura de gestión de acceso URL modificada en el cortafuegos.

1. Seleccione **Administrar** > **configuración** > **Servicios de seguridad** > **URL Administración de acceso** > **Páginas de respuesta**.
2. Haga clic en la página de bloqueo de búsqueda segura de Gestión de acceso URL. Aparece un cuadro de diálogo con la opción **Choose File (Elegir archivo)**.
3. Seleccione el archivo de página de bloqueo de búsqueda segura que editó anteriormente y haga clic en **Save (Guardar)**.

STEP 6 | Cree una categoría de URL personalizada para los motores de búsqueda compatibles.

En el siguiente paso, configurará el cortafuegos para descifrar el tráfico a esta categoría personalizada.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)**.
2. En **Access Control (Control de acceso)**, para categorías de URL personalizadas, **Add Category (Añadir categoría)**.
3. Introduzca un nombre en **Name (Nombre)** para la categoría, como **`SearchEngineDecryption`**.
4. Para el **Type (Tipo)** de la categoría de URL personalizada, seleccione **URL List (Lista de URL)**.
5. En **Items (Elementos)**, seleccione **Add (Añadir)** las siguientes entradas a la lista de URL:
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
6. Seleccione **Save (Guardar)** la categoría personalizada.
7. Configure el acceso al sitio para la nueva categoría de URL personalizada.
   1. En Perfiles de gestión de acceso URL, seleccione el perfil que configuró anteriormente.
   2. En Control de acceso, seleccione la nueva categoría de URL personalizada. Esta aparece en la sección Categorías de URL personalizadas, encima de Listas de URL dinámicas externas y Categorías predefinidas.
   3. Establezca **Site Access (Acceso al sitio)** en **allow (permitir)**.
   4. Haga clic en **Save (Guardar)** para guardar sus cambios.

STEP 7 | Configure el descifrado del proxy SSL de reenvío.

Dado que la mayoría de los motores de búsqueda cifran los resultados de búsqueda, debe habilitar el descifrado del proxy SSL de reenvío para que el cortafuegos pueda inspeccionar el tráfico de búsqueda y detectar la configuración de búsqueda segura.

En **Services and URLs (Servicios y URL)** de la regla de política de descifrado, haga clic en **Add URL Categories (Añadir categorías de URL)**. A continuación, seleccione la categoría de URL personalizada que creó anteriormente. Las nuevas categorías personalizadas se encuentran en la parte superior de la lista.

Debe **Save (Guardar)** la regla de la política de descifrado.

STEP 8 | Seleccione **Push Config (Enviar configuración)** para activar los cambios.

STEP 9 | Compruebe la configuración de la aplicación de búsquedas seguras.

Desde un ordenador detrás de un cortafuegos, abra un navegador y realice una búsqueda utilizando Bing, Yahoo o Yandex. Luego, utilice uno de los siguientes métodos para verificar su configuración:

- Examine la cadena de consulta de la URL para parámetros de búsqueda segura. La configuración de búsqueda segura para proveedores de búsqueda enumera el parámetro de búsqueda segura adjunto a cada URL de consulta de búsqueda.
- Vaya a la configuración de búsqueda segura de un motor de búsqueda compatible y verifique que la preferencia de SafeSearch seleccionada sea el nivel más estricto (**Strict (Estricto)** en la mayoría de los casos).

Forzar búsqueda segura estricta (PAN-OS y Panorama)

STEP 1 | Asegúrese de que el cortafuegos ejecuta la versión de publicación de contenido 475 o posterior.

1. Seleccione **Device** > **Dynamic Updates** (Dispositivo > Actualizaciones dinámicas).
2. Compruebe la sección **Aplicaciones y amenazas** para determinar qué actualización se está ejecutando.
3. Si el cortafuegos no está ejecutando la actualización requerida o posterior, haga clic en **Check Now (Comprobar ahora)** para recuperar una lista de actualizaciones disponibles.
4. Busque la actualización requerida y haga clic en **Download (Descargar)**.
5. Cuando finalice la descarga, haga clic en **Install (Instalar)**.

STEP 2 | Habilite la aplicación de búsquedas seguras en un perfil de filtrado de URL.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **URL Filtering (Filtrado de URL)**.
2. Seleccione un perfil existente para modificarlo o duplique el perfil predeterminado para crear un nuevo perfil.
3. En la pestaña **URL Filtering Settings (Configuración de URL Filtering)**, seleccione **Safe Search Enforcement (Aplicación de búsquedas seguras)**.

STEP 3 | (Opcional) Restrinja los motores de búsqueda a los que pueden acceder los usuarios finales en el mismo perfil de filtrado de URL.

1. En la pestaña **Categories (Categorías)**, **Search (Busque)** ( ) la categoría **search-engines (motores de búsqueda)**
2. Establezca el acceso al sitio para la categoría **search-engines (motores de búsqueda)** en **block (bloquear)**.

   En un paso posterior, creará una categoría de URL personalizada (Tipo de lista de URL) con los motores de búsqueda que desea permitir.
3. Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 4 | Aplique el perfil de URL Filtering a las reglas de la política de seguridad que permiten el tráfico de los clientes de la zona de confianza a Internet.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**. A continuación, haga clic en la regla a la que desea aplicar el perfil de URL Filtering.
2. En la pestaña **Actions (Acciones)**, busque Configuración de perfil. Para **Profile Type (Tipo de perfil)**, seleccione **Profiles (Perfiles)**. Aparece una lista de perfiles.
3. Para el perfil de **URL Filtering (Filtrado de URL)**, seleccione el perfil que creó anteriormente.
4. Haga clic en **OK (Aceptar)** para guardar la regla de la política de seguridad.

STEP 5 | Edite la página de bloqueo de búsqueda segura de filtrado de URL, reemplazando el código existente con JavaScript para reescribir las URL de las consultas de búsqueda.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** > **URL Filtering Safe Search Block Page (Página de bloque de búsqueda segura de filtrado de URL)**.
2. Seleccione **Predefinido** y, a continuación, haga clic en **Exportar** para guardar el archivo localmente.
3. Utilice un editor HTML y sustituya todo el texto de la página de bloqueo existente con el siguiente texto. Luego, guarde el archivo.

```
<html> <head> <title>Búsqueda bloqueada</title> <meta http-
equiv="Content-Type" content="text/html; charset=utf-8">
 <meta http-equiv="pragma" content="no-cache"> <meta
 name="viewport" content="initial-scale=1.0"> <style> #content
 { border:3px solid#aaa; background-color:#fff; margin:1.5em;
 padding:1.5em; font-family:Tahoma,Helvetica,Arial,sans-serif;
 font-size:1em; } h1 { font-size:1.3em; font-weight:bold;
 color:#196390; } b { font-weight:normal; color:#196390; }
 </style> </head> <body bgcolor="#e7e8e9"> <div id="content">
 <h1>Búsqueda bloqueada</h1> <p> <b>Usuario:</b> <user/>
 </p> <p>Los resultados de búsqueda se han bloqueado porque
 la configuración de búsqueda no se ajusta a la política
 de la empresa. Para continuar, actualice la configuración
 de búsqueda para que Búsqueda segura se establezca en la
 configuración más estricta. Si actualmente ha iniciado
 sesión en su cuenta, bloquee también Búsqueda segura e
 intente su búsqueda nuevamente.</p> <p> Para obtener más
 información, consulte: <a href="<ssurl/>"> <ssurl/> </a> </p>
 <p id="java_off"> Habilite JavaScript en su navegador.<br></
p> <p><b>Póngase en contacto con el administrador del
 sistema si cree que este mensaje es un error.</b></p> </
div> </body> <script> Tome la URL que está en el navegador.
 var s_u = location.href; bing // Coincide con las barras
 diagonales al principio, cualquier cosa, luego ".bing."
 luego cualquier cosa seguida de una barra diagonal no
 expansiva. Hopefully the first forward slash. var b_a
 = /^.*\/\/(.+\.bing\..+?)\//.exec(s_u); if (b_a) { s_u
 = s_u + "&adlt=strict"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; } //
yahoo // Matches the forward slashes in the beginning,
 anything, then ".yahoo."" then anything followed by
```



```
 a non greedy slash. Esperemos que la primera barra
 hacia adelante. var y_a = /^.*\/\/(.+\.yahoo\..
+?)\//.exec(s_u); if (y_a) { s_u = s_u.replace(/&vm=p/
ig,""); s_u = s_u + "&vm=r"; window.location.replace(s_u);
 document.getElementById("java_off").innerHTML =
 'You are being redirected to a safer search!'; }
 document.getElementById("java_off").innerHTML = ' '; </
script> </html>
```

STEP 6 | Importe la página editada de bloqueo de búsqueda segura de filtrado de URL al cortafuegos.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** > **URL Filtering Safe Search Block Page (Página de bloqueo de búsqueda segura de filtrado de URL)**.
2. Haga clic en **Import (Importar)**. Luego, **busque** el archivo de la página de bloqueo o introduzca la ruta y el nombre del archivo en el campo **Import File (Importar archivo)** .
3. (Opcional) Para **Destination (Destino)**, seleccione el sistema virtual en el que se usará o **shared (compartirá)** la página de inicio de sesión para que esté disponible para todos los sistemas virtuales.
4. Haga clic en **OK (Aceptar)** para importar el archivo.

STEP 7 | Cree una categoría de URL personalizada para los motores de búsqueda compatibles.

En el siguiente paso, configurará el cortafuegos para descifrar el tráfico a esta categoría personalizada.

1. Seleccione **Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)** y luego **Add (Añadir)** para añadir una categoría personalizada.
2. Introduzca un nombre en **Name (Nombre)** para la categoría, como **`SearchEngineDecryption`**.
3. Seleccione **Add (Añadir)** para añadir las siguientes entradas a la lista **Sites (Sitios)**:
   - **`www.bing.*`**
   - **`search.yahoo.*`**
   - **`yandex.com.*`**
4. Haga clic en **OK (Aceptar)** para guardar la categoría de URL personalizada.

STEP 8 | Configure el descifrado del proxy SSL de reenvío.

Dado que la mayoría de los motores de búsqueda cifran los resultados de búsqueda, debe habilitar el descifrado del proxy SSL de reenvío para que el cortafuegos pueda inspeccionar el tráfico de búsqueda y detectar la configuración de búsqueda segura.

En la pestaña **Service/URL Category (Categoría de servicio/URL)** de la regla de política de descifrado, seleccione **Add (Añadir)** la categoría de URL personalizada que creó anteriormente. Después, haga clic en **OK (Aceptar)**.

STEP 9 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

STEP 10 | Compruebe la configuración de la aplicación de búsquedas seguras.

Desde un ordenador detrás de un cortafuegos, abra un navegador y realice una búsqueda usando Bing o Yahoo. Luego, utilice uno de los siguientes métodos para verificar que su configuración funcione según lo previsto:

- Examine la cadena de consulta de la URL para parámetros de búsqueda segura. La configuración de búsqueda segura para proveedores de búsqueda enumera el parámetro de búsqueda segura adjunto a cada URL de consulta de búsqueda.
- Vaya a la configuración de Búsqueda segura del motor de búsqueda y verifique que la preferencia de búsqueda segura, SafeSearch, seleccionada sea el nivel más estricto (**Strict (Estricto)** en el caso de Bing).

Usar SafeSearch transparente en Prisma Access

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) Si desea utilizar esta función en su entorno de Prisma Access, póngase en contacto con su equipo de cuenta para obtener más información.	❑ Una implementación de Prisma Access que ejecuta una versión mínima de 4.1 ❑ Licencia de Prisma Access

Prisma Access le permite resolver las consultas del motor de búsqueda de los usuarios móviles al portal SafeSearch del motor de búsqueda realizando una asignación de FQDN a IP. Utilice SafeSearch transparente como alternativa a la implementación de SafeSearch estricta cuando el tráfico no se puede descifrar (por ejemplo, en una tienda que proporciona acceso a internet para invitados) y desea evitar que los usuarios con dispositivos no gestionados, incluidos los dispositivos de visualización, busquen material restringido, inapropiado u ofensivo.

- Strata Cloud Manager
- Panorama

Usar SafeSearch transparente en Prisma Access (Strata Cloud Manager)

Para configurar el soporte de SafeSearch transparente para Prisma Access en Strata Cloud Manager, complete los siguientes pasos. Puede configurar SafeSearch transparente para redes remotas o usuarios móviles de GlobalProtect.

STEP 1 | Elija el tipo de implementación (usuarios móviles o redes remotas) para el que desea configurar SafeSearch.

- Para usuarios móviles: implementaciones de GlobalProtect, vaya a **Manage (Gestionar)** > **Service Setup (Configuración del servicio)** > **Mobile Users (Usuarios móviles)**; luego,

seleccione **GlobalProtect Setup (Configuración de GlobalProtect)** > **Infrastructure Settings (Configuración de infraestructura)**.

Si está usando Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Mobile Users (Usuarios móviles)**; luego, seleccione **GlobalProtect Setup (Configuración de GlobalProtect)** > **Infrastructure Settings (Configuración de infraestructura)**.

- Para implementaciones de redes remotas, vaya a **Manage (Gestionar)** > **Service Setup (Configuración de servicio)** > **Remote Networks (Redes remotas)**.

  Si está usando Strata Cloud Manager, vaya a **Workflows (Flujos de trabajo)** > **Prisma Access Setup (Configuración de Prisma Access)** > **Remote Networks (Redes remotas)**.

STEP 2 | Seleccione **Advanced Settings (Configuración avanzada)**.

STEP 3 | Utilice **Static Entries (Entradas estáticas)** para resolver FQDN en direcciones IP específicas.

STEP 4 | Introduzca un **Name (Nombre)** único para la regla de entrada estática, el **FQDN** para el motor de búsqueda y la **Address (Dirección)** IP de SafeSearch del motor de búsqueda donde debe dirigirse la solicitud de FQDN.

Usar SafeSearch transparente en Prisma Access (Panorama)

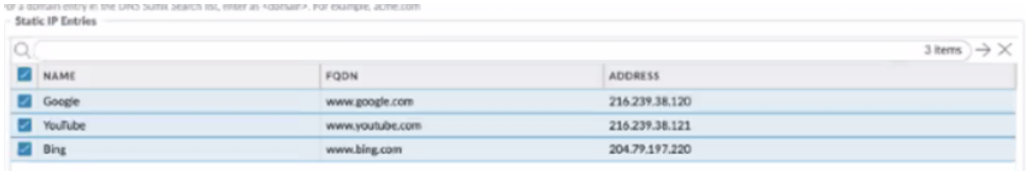
Para configurar el soporte de SafeSearch transparente para Prisma Access en Panorama, complete los siguientes pasos. Puede configurar SafeSearch transparente para redes remotas o usuarios móviles de GlobalProtect.

STEP 1 | Elija el tipo de implementación (redes remotas o usuarios móviles) para el que desea configurar SafeSearch.

- Para las implementaciones de Mobile Users—GlobalProtect, vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Mobile Users—GlobalProtect (Usuarios móviles—GlobalProtect)**, seleccione **Configure (Configurar)** en el área de **Onboarding (Incorporación)**; luego, seleccione **Network Services (Servicios de red)**.
- Para implementaciones de Remote Network (Redes remotas), vaya a **Panorama** > **Cloud Services (Servicios en la nube)** > **Configuration (Configuración)** > **Remote Networks (Redes remotas)**, haga clic en el engranaje para modificar la **Settings (Configuración)**; luego, seleccione **DNS Proxy (Proxy DNS)**.

STEP 2 | Introduzca **Static IP Entries (Entradas IP estáticas)** introduciendo un **Name (Nombre)** único para la regla de entrada estática, el **FQDN** para el motor de búsqueda y la **Address**

(Dirección) IP de SafeSearch del motor de búsqueda a la que debe dirigirse la solicitud FQDN.



Integrar con un proveedor de aislamiento remoto del navegador de terceros

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	❑ Licencia de Advanced URL Filtering ***Nota:*** *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Si bien es la acción más segura, bloquear sitios desconocidos y peligrosos puede afectar la experiencia y la productividad de los usuarios. El aislamiento remoto del navegador (RBI) redirige a los usuarios desde sitios desconocidos o peligrosos a un entorno aislado alojado por un proveedor de RBI. El sitio web se presenta al usuario y este puede ver los recursos que necesita, sin acceder directamente al sitio desconocido o peligroso desde su endpoint.

Prisma Access se integra fácilmente con los proveedores de RBI para este tipo de redireccionamiento del navegador. En solo uno o dos pasos, puede elegir el proveedor de RBI con el que desea integrarse y luego elegir las categorías de URL que desea dirigir al entorno alojado del proveedor de RBI.

Además de los proveedores de RBI de terceros, el Aislamiento remoto del navegador*, o Remote Browser Isolation, (RBI) de Palo Alto Networks está disponible para integrarse de forma nativa con Prisma Access. A diferencia de otras soluciones de aislamiento, RBI utiliza tecnologías de aislamiento de nueva generación para ofrecer experiencias casi nativas a los usuarios que acceden a sitios web sin por ello comprometer la seguridad.*

Aquí están los proveedores del RBI con lo que Prisma Access se integra: algunos proveedores pueden requerir que añada detalles del entorno RBI (como una URL personalizada o una identificación de inquilino) a Strata Cloud Manager para configurar la integración:

- **RBI de Palo Alto Networks**

  Para integrarse con RBI de Palo Alto Networks, deberá configurar el aislamiento remoto del navegador.
- **Auténtico8**

  Para integrarse con Authentic8, tenga a mano la URL personalizada del entorno Authentic8 RBI.
- **Proofpoint**

  Para integrarse con Proofpoint, prepárese para elegir utilizar el entorno de producción de Proofpoint o PoC para RBI.
- **Ericom**

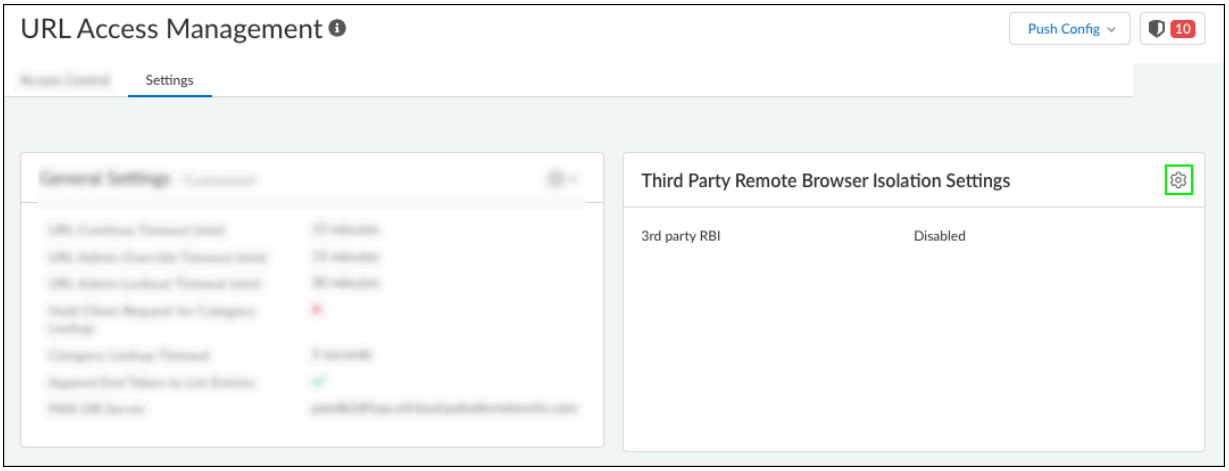
  Para integrarse con Ericom, tenga a mano el ID de inquilino para el entorno de Ericom RBI.
- **Menlo Security**

  No necesita realizar ninguna configuración para el entorno de Menlo Security RBI; todo lo que necesita hacer es habilitar la integración.

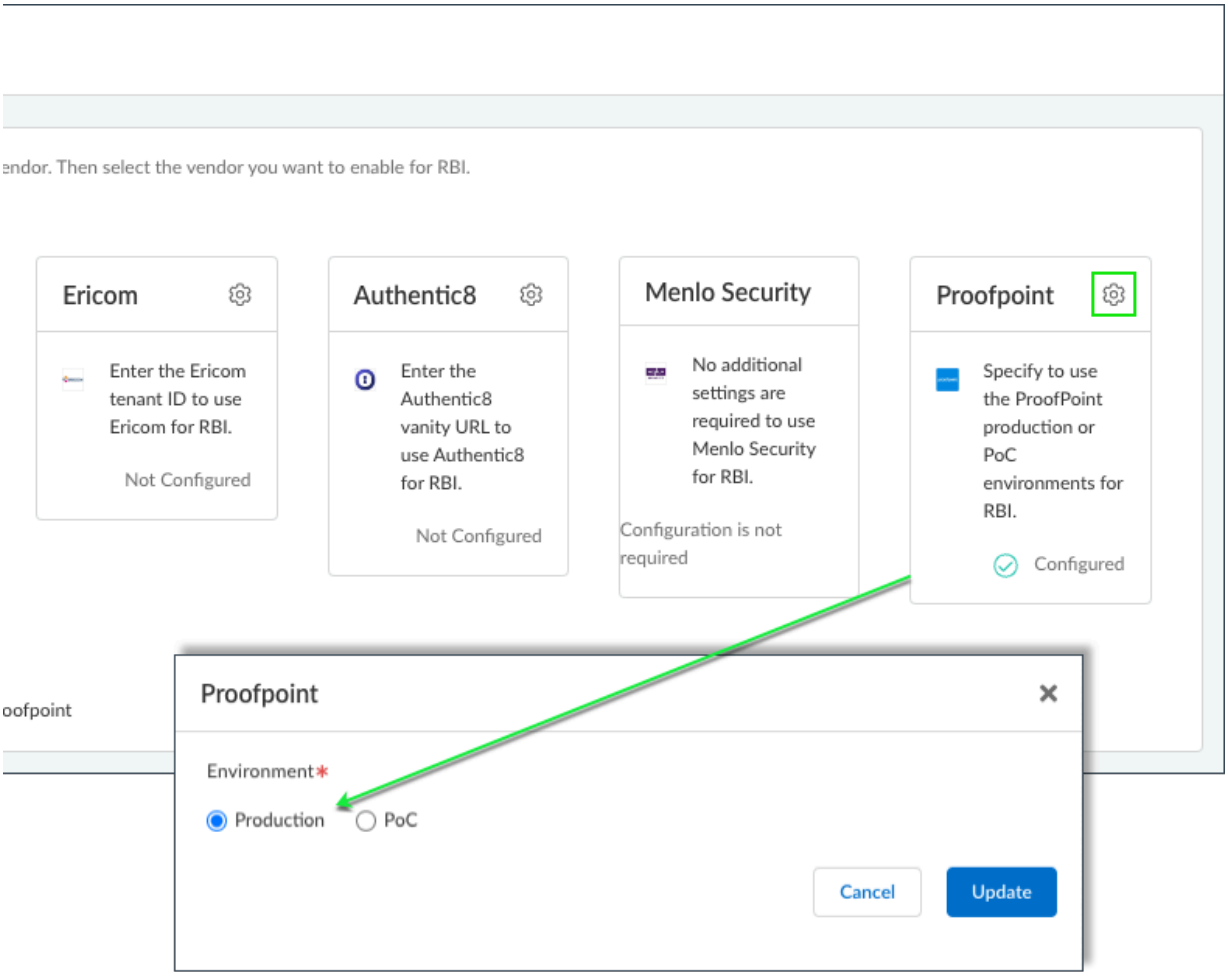
Aquí le mostramos cómo añadir su proveedor externo de RBI a Strata Cloud Manager y especifique las categorías de URL que redirigirán a los usuarios al entorno RBI.

STEP 1 | Configurar el Aislamiento remoto del navegador (RBI).

- Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **URL Access Management (Gestión de acceso URL)** > **Settings (Configuración)** y abra la **Third Party Remote Browser Isolation Settings (Configuración de aislamiento remoto del navegador de terceros)** de .
- **SI USTED ES UN ADMINISTRADOR DE SEGURIDAD WEB**: Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **Web Security (Seguridad web)** > **Threat Management (Gestión de amenazas)** y abra la **Third Party Remote Browser Isolation Settings (Configuración de aislamiento remoto del navegador de terceros)** de .

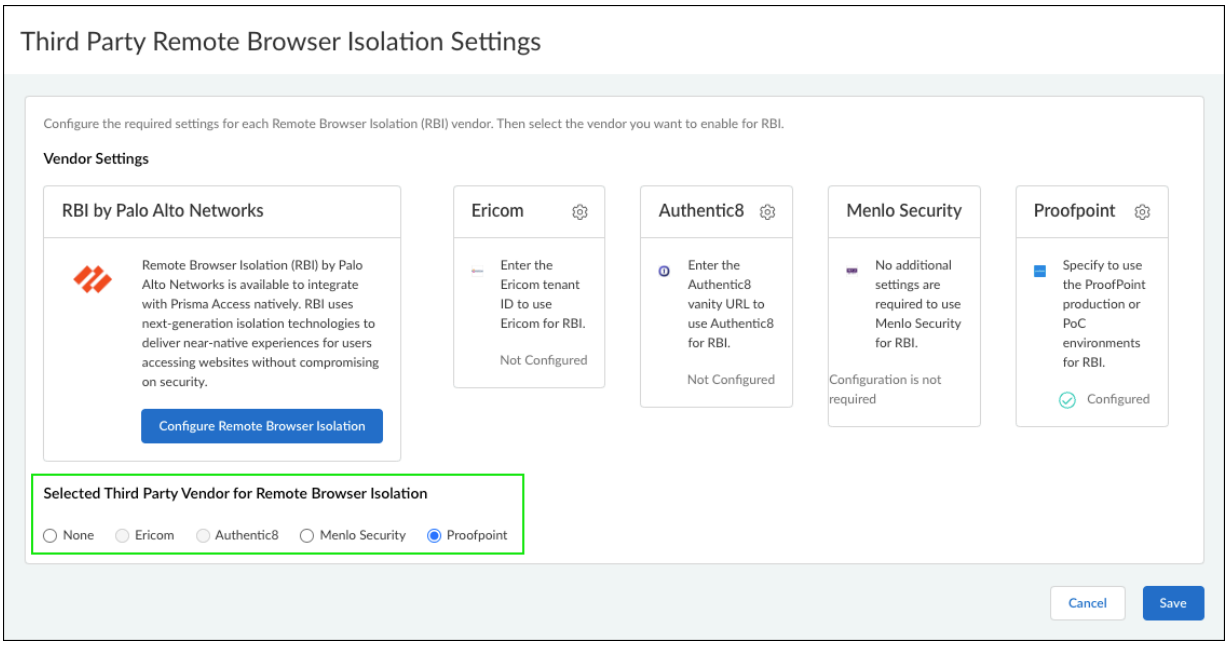


STEP 2 | Verifique si su RBI requiere que especifique el entorno RBI que desea utilizar; si es así, introduzca la configuración requerida.



STEP 3 | Luego, seleccione el proveedor de RBI de terceros que desea habilitar y **Save (Guardar)**. ¡Eso es todo! La próxima vez que tenga que **Push Config (Enviar configuración)**, su proveedor de RBI se integrará con Prisma Access.

*También puede **configurar el aislamiento remoto del navegador** si ya compró y activó la licencia de RBI de Palo Alto Networks. Sin embargo, no se puede utilizar RBI de Palo Alto Networks y un proveedor externo de RBI para el aislamiento. Si elige utilizar RBI de Palo Alto Networks, seleccione **None (Ninguno)**, de lo contrario, seleccione un proveedor externo de RBI en **Selected Third Party Vendor for Remote Browser Isolation (Proveedor externo seleccionado para aislamiento remoto del navegador**.*

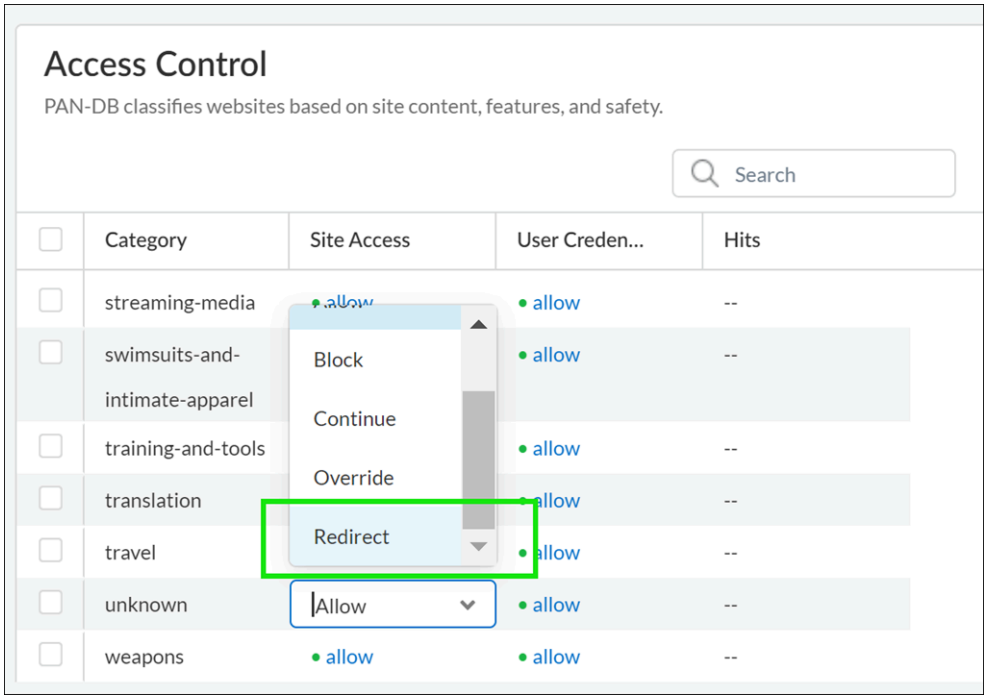


STEP 4 | Ahora, especifique las categorías de URL que redirigirán a los usuarios al entorno RBI.

Vaya a **URL Access Management > Access Control (Gestión de acceso URL > Control de acceso)** y añada o modifique un **URL Access Management Profile (Perfil de gestión de acceso URL)**.

En la configuración **Access Control (Control de acceso)**, actualice el **Site Access (Acceso a sitio)** a **Redirect (Redirigir)**.

La nueva acción **Redirect (Redirigir)** redirige a los usuarios al entorno RBI en lugar de presentarles una página de bloqueo.



Supervisión

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Supervisar la actividad web en su red es esencial para proteger su organización y garantizar la eficacia de su política de filtrado de URL. Las plataformas de Palo Alto Networks generan registros detallados que sirven como una fuente para paneles e informes. Puede personalizar logs, paneles e informes para satisfacer sus necesidades específicas de supervisión y generación de informes. Si es necesario, puede solicitar cambios de categoría de URL de logs de filtrado de URL. Utilice la información que ofrecen nuestras herramientas de supervisión para ajustar las reglas de políticas de acceso web, y analizar y tomar medidas ante cualquier actividad sospechosa.

Las funciones Creación de logs del encabezado HTTP y Solo página de contenedor de logs ofrecen control sobre el volumen y los detalles del log. La creación de logs del encabezado HTTP aumenta la granularidad de los logs. Registrar los logs del acceso de usuarios de la página principal únicamente reduce el número de logs generados.

Explore los siguientes temas para obtener más información sobre las herramientas y funciones de supervisión de la actividad web.

- Supervisar la actividad web
- Registro solo de las páginas que visita un usuario
- Creación de logs del encabezado HTTP
- Solicitud para cambiar la categoría de una URL

Supervisar la actividad web

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Puede ver varios paneles, informes y logs para revisar y analizar la actividad web en su red. Por ejemplo, en los cortafuegos de nueva generación de PAN-OS, los registros e informes de filtrado de URL de Application Command Center (ACC) muestran toda la actividad web del usuario para las categorías de URL establecidas en **alert (alerta)**, **block (bloquear)**, **continue (continuar)** o **override (cancelar)**. Al supervisar la actividad del usuario con las siguientes herramientas, puede obtener una mejor comprensión de la actividad web de su base de usuarios y determinar las reglas de la política de acceso web adecuadas.

Zero Trust	Formas de ver la actividad web del usuario
PAN-OS y Panorama	• Centro de control de aplicaciones (ACC) • Widgets de actividad de red • Logs de URL Filtering • Informes de filtrado de URL
Prisma Access	• Logs • Insights • Autonomous DEM • Actividad

- Strata Cloud Manager
- PAN-OS y Panorama

Supervisar la actividad web (Strata Cloud Manager)

Independientemente de la interfaz que esté utilizando para gestionar Prisma Access (Panorama o Strata Cloud Manager), el panel Actividad de Strata Cloud Manager proporciona una vista completa de lo que está sucediendo en su red. Varios paneles componen el panel Actividad,

que está disponible en el Strata Cloud Manager y la aplicación Device Insights. También puede compartir datos de Actividad con otros usuarios de su organización.

Los siguientes paneles interactivos le ayudan a supervisar y analizar la actividad web en su red:

- **Información sobre amenazas**: una vista holística de todas las amenazas que Advanced URL Filtering y otros servicios de seguridad de Palo Alto Networks detectaron y bloquearon en su red. Puede ver las tendencias de amenazas, las aplicaciones afectadas, los usuarios y las reglas de la política de seguridad que permiten o bloquean amenazas.
- **Visor de logs** : los logs proporcionan una pista de auditoría para los eventos del sistema, la configuración y la red. Vaya de un panel de actividad a sus logs para obtener detalles e investigar los hallazgos.
- **Uso de las aplicaciones** : vea una descripción general de las aplicaciones de su red, incluido su riesgo, estado de autorización, ancho de banda consumido y los principales usuarios de estas aplicaciones.
- **Resumen ejecutivo** (**Filtrado de URL**): vea qué categorías de URL representan la mayor parte de la actividad web en su red, las 10 URL maliciosas principales y las 10 URL de alto riesgo principales.
- **Actividad del usuario**: Vea los patrones de navegación de los usuarios individuales: los sitios que visitan con más frecuencia, los sitios con los que transfieren datos y los intentos de acceder a sitios de alto riesgo. Los datos de los logs de Filtrado de URL y Motor de identidad en la nube permiten esta visibilidad.

  - *Para acceder a los datos de actividad de los usuarios y compartir informes de forma fácil y segura, recomendamos* activar *y* configurar el Motor de identidad en la nube.

Visibilidad adicional y métodos de supervisión:

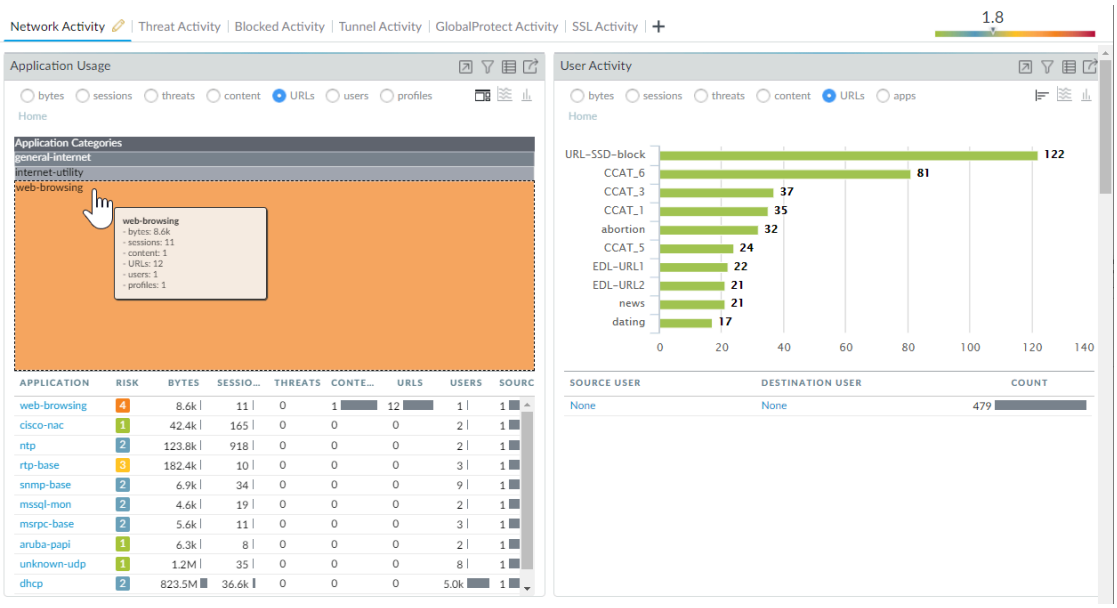
- El panel Informes incluye opciones para programar la entrega de informes o descargar y compartir un informe en cualquier momento para verlo sin conexión.
- También puede hacer lo siguiente: Buscar un artefacto de seguridad (una dirección IP, un dominio, una URL o un hash de archivo) para interactuar con los datos solo para ese artefacto, extraídos de los hallazgos de su red y la inteligencia de amenazas global.

1. Abrir un panel de actividad.
   - Seleccione **Activity (Actividad)** > **Threat Insights | Application Usage | User Activity | Executive Summary (Información sobre amenazas | Uso de las aplicaciones | Actividad del usuario | Resumen ejecutivo)**.

     Para ver el resumen ejecutivo del filtrado de URL, deberá hacer clic en la pestaña Filtrado de URL cuando esté en el panel.
   - Para acceder al Visor de logs, seleccione **Activity (Actividad)** > **Logs (Logs)** > **Log Viewer (Visor de logs)**.
2. Descargar, compartir y programar informes de actividad.

Supervisar la actividad web (PAN-OS & Panorama)

- Para obtener una vista rápida de las categorías más comunes a las que acceden los usuarios de su entorno, seleccione los widgets de **ACC**. La mayoría de widgets de la pestaña **Network Activity (Actividad de red)** le permiten ordenar las URL. Por ejemplo, en el widget Uso de aplicación puede ver que la categoría de red es la categoría a la que más se accede, seguida del túnel cifrado y ssl. También puede ver la lista de **Threat Activity** y **Blocked Activity** ordenada en URL.



Vea los logs y configure las opciones de log:

- En el ACC, puede pasar directamente a los logs ( ) o seleccionar **Monitor (Supervisar)** > **Logs** > **URL Filtering**.

  La acción del log para cada entrada depende de la configuración de acceso al sitio que define para la categoría correspondiente:

  - **Log de alerta:** en este ejemplo, a la categoría computer-and-internet-info (Información de ordenador e internet) se le asignó la acción alert (crear alerta).

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/16 14:10:53	computer-and-internet-info	outlook.office36...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	outlook-web-online	alert

  - **Log de bloqueo:** en este ejemplo, a la categoría insufficient-content (contenido insuficiente) se le asignó la acción continue (continuar). Si a la categoría se le hubiese asignado la acción block (bloquear), el log Action (Acción) sería block-url (bloquear URL).

	RECEIVE TIME	CATEGORY	URL	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/08 18:47:49	insufficient-content	munchkin.mark...	pm wifi	UNTRUST	[redacted]	[redacted]	[redacted]	ssl	block-continue

  - **Log de alerta en el sitio web cifrado:** en este ejemplo, la categoría es private-ip-addresses (direcciones IP privadas) y la aplicación es web-browsing (navegación web). Además, este log indica que el cortafuegos descifró este tráfico.

	RECEIVE TIME	CATEGORY	URL	DECRYPTED	FROM ZONE	TO ZONE	SOURCE	SOURCE USER	DESTINATION	APPLICATION	ACTION
	2020/04/09 14:11:29	private-ip-addresses	[redacted]/Updates/Updat...	yes	TRUST	UNTRUST	192.168.58.3	[redacted]	[redacted]	web-browsing	alert

- El veredicto de aprendizaje automático en línea [local] (PAN-OS 10.0/10.1) y el veredicto de categorización en línea [local y en la nube] (PAN-OS 10.2 y posteriores) indican el veredicto determinado por los analizadores basados en el aprendizaje automático en línea.

  - El veredicto de aprendizaje automático en línea se aplica a las URL que se han categorizado mediante el aprendizaje automático en línea de URL Filtering operado localmente en PAN-OS 10.0/10.1.

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE ML VERDICT	ACTION	URL
	10/11 17:32:10	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
	10/11 14:15:14	malware	malware	phishing	block	hisperfectlight.com/downloads/etipa/login.php?cmd=login_submit&id=2cf35df3...
	04/30 15:19:30	medium-risk	medium-risk,unknown	malicious-javascript	block	130.127.24.16/0x39814f84/448d21c8e396e8f4e0eb75de69d6473e033422b...

    Los siguientes veredictos están disponibles:

    - **Phishing**: contenido de ataques de phishing detectados por el ML en línea local.
    - **Malicious-javascript**: contenido de javascript malicioso detectado por el ML en línea local.
    - **Desconocido**: se clasificó la URL y se determinó que el contenido era benigno.
  - El veredicto de categorización en línea se aplica a las URL que se han clasificado utilizando el Aprendizaje automático en línea de URL Filtering operado localmente (que pasó a llamarse Categorización en línea local en PAN-OS 10.2) así como la Categorización en línea

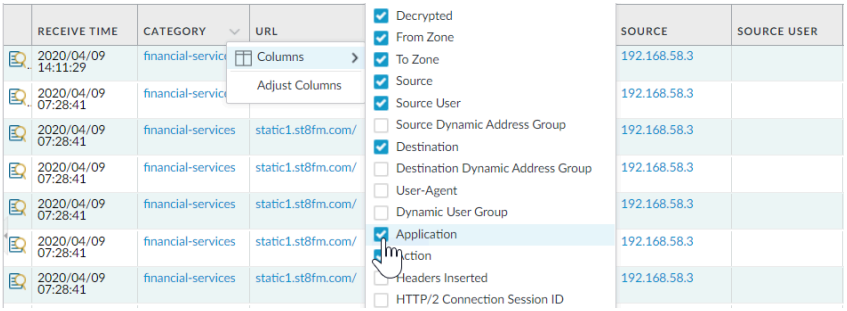
en la nube, que opera en la nube de Advanced URL Filtering. El tipo específico de ataque se especifica en la columna de categoría del log.

	RECEIVE TIME	CATEGORY	URL CATEGORY LIST	INLINE CATEGORIZATI... VERDICT	ACTION	URL
	08/16 15:16:58	computer-and-internet-info	computer-and-internet-info,high-risk	N/A	alert	mlav.testpanw.com/js.html
	08/16 15:16:58	phishing	computer-and-internet-info,high-risk	local	block	mlav.testpanw.com/phishing.html
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com/test-inline-content-analysis-phishing
	08/16 15:14:58	phishing	phishing,real-time-detection	cloud	block-url	urlfiltering.paloaltonetworks.com:80/test-inline-content-analysis-phishing

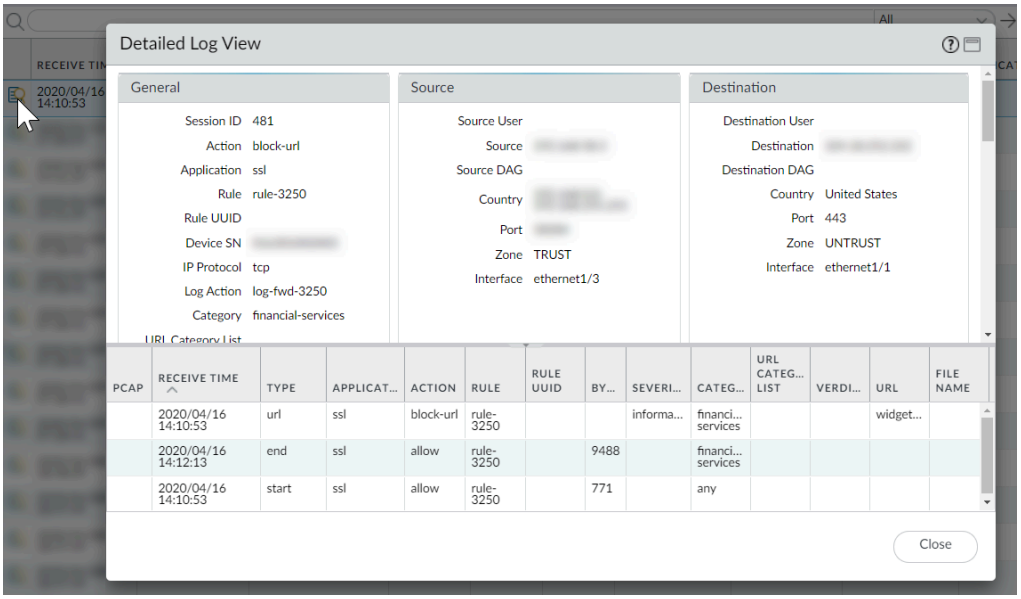
Los siguientes veredictos están disponibles:

- **Local**: contenido malicioso detectado mediante la categorización en línea local.
- **Nube**: contenido malicioso detectado mediante el motor de categorización en línea en la nube ubicado en la nube de Advanced URL Filtering.
- **N/D**: los motores de categorización en línea locales o en la nube no analizaron la URL.

- También puede añadir otras columnas a su vista de log de filtrado de URL, como las zonas de origen y destino, el tipo de contenido y si se realizó o no una captura de paquetes. Para modificar qué columnas mostrar, haga clic en la flecha hacia abajo en cualquier columna y seleccione el atributo que debe mostrarse.

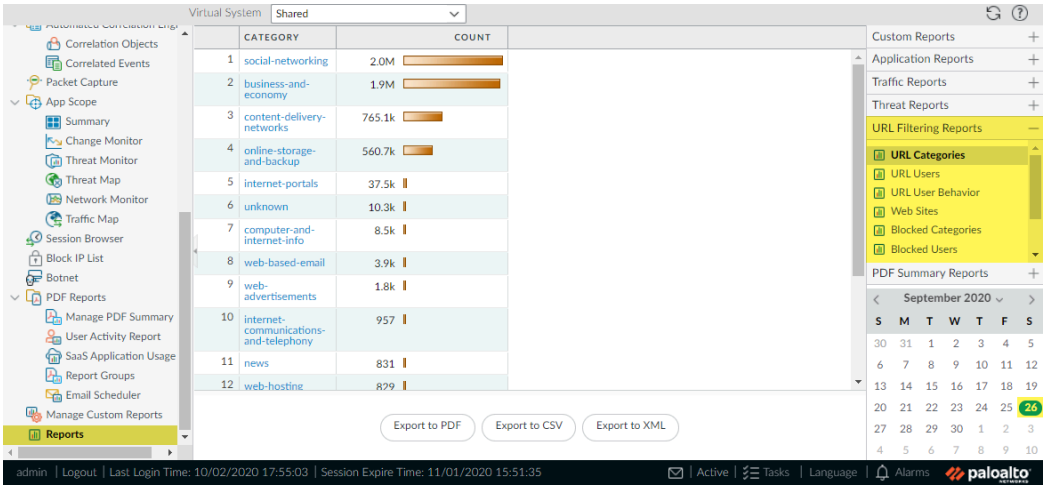


- Para ver la información detallada completa del log y/o solicitar un cambio de categoría para la URL específica a la que se accedió, haga clic en el icono de información detallada del log en la primera columna del log.



- Genere informes de filtrado de URL predefinidos en las categorías de URL, los usuarios de URL, los sitios web a los que se accede, las categorías bloqueadas, etc.

  Seleccione **Monitor (Supervisar)** > **Reports (Informes)** y, en la sección **URL Filtering Reports (Informes de filtrado de URL)**, seleccione uno de los informes. Los informes abarcan un período de 24 horas en la fecha del calendario que selecciona. También puede exportar el informe a PDF, CSV o XML.



Visualización del informe de actividad del usuario

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager)	☐ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada)

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Este informe proporciona un método rápido para visualizar la actividad de un usuario o grupo y también ofrece la opción de visualizar la actividad de tiempo de exploración.

- Strata Cloud Manager
- PAN-OS y Panorama

Ver el informe de actividad del usuario (Strata Cloud Manager)

Ya sea que esté usando Panorama o Strata Cloud Manager para gestionar Prisma Access, puede ir a la aplicación de Strata Cloud Manager para generar un informe de actividad del usuario. En la aplicación, vaya a **Activity (Actividad)** para encontrar el panel de **User Activity Report) Informe de actividad del usuario**. El acceso a los datos de actividad del usuario requiere un inquilino del motor de identidad en la nube activo.

STEP 1 | Active el motor de identidad en la nube.

STEP 2 | Configure el motor de identidad en la nube

STEP 3 | Configure un informe de actividad del usuario

1. Seleccione **Activity (Actividad)** > **User Activity (Actividad del usuario)**.
2. Debe **Enter Username (Introducir el nombre de usuario)** para generar un informe para una persona.
3. Seleccione el **Type (Tipo)** de servidor:
   - Seleccione **User (Usuario)** para generar un informe para una persona.
   - Seleccione **Group (Grupo)** para seleccionar un grupo de usuarios.

   Debe habilitar User-ID *para poder seleccionar nombres de usuario o grupo. Si User-ID no se ha configurado, puede seleccionar el tipo **User (Usuario)** e introducir la dirección IP del equipo del usuario.*
4. Introduzca el **Username/IP Address (Nombre de usuario/dirección IP)** de un informe de usuario o introduzca el nombre de grupo de un informe de grupo de usuarios.
5. Seleccione el periodo de tiempo. Puede seleccionar un período de tiempo existente o seleccionar **Custom (Personalizado)**.
6. Seleccione la casilla de verificación **Include Detailed Browsing (Incluir exploración detallada)** para que se incluya información de exploración en el informe.

STEP 4 | Ejecute el informe.

1. Haga clic en **Run now (Ejecutar ahora)**.
2. Cuando el cortafuegos termine de generar el informe, haga clic en uno de los enlaces para descargarlo:
   - Haga clic en **Download User Activity Report (Descargar informe de actividad del usuario)** para descargar una versión en PDF del informe.
   - Haga clic en **Download URL Logs (Descargar logs de URL)** para descargar un archivo CSV de las entradas de log correspondientes.
3. Tras descargar el informe, haga clic en **Cancel (Cancelar)**.
4. Si desea guardar la configuración del informe de actividad del usuario para poder ejecutar el mismo informe más tarde, haga clic en **OK (Aceptar)**; de lo contrario, haga clic en **Cancel (Cancelar)**.

STEP 5 | Vea el informe de actividad del usuario abriendo el archivo que descargó. La versión PDF del informe muestra el usuario o el grupo en el que basó el informe, el período de tiempo del informe y un índice:

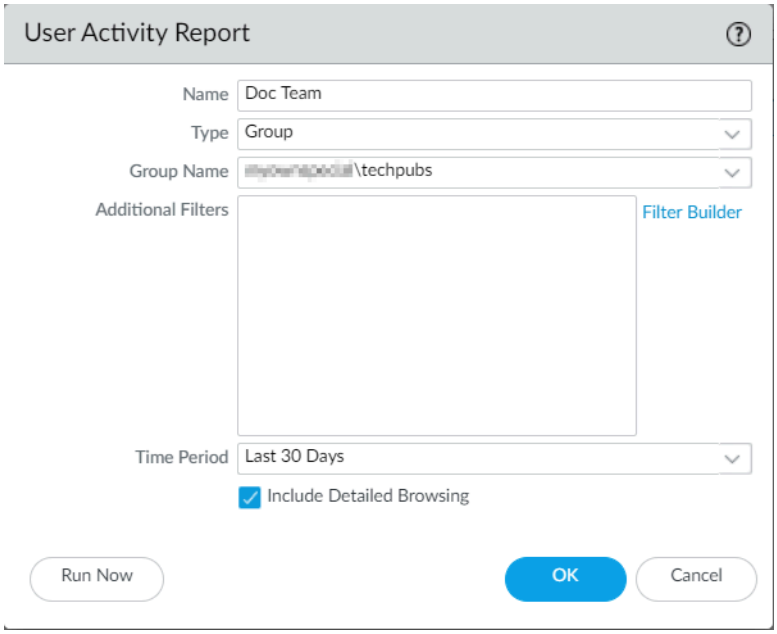
STEP 6 | Haga clic en un elemento del índice para ver los detalles del informe. Por ejemplo, haga clic en **Traffic Summary by URL Category (Resumen de tráfico por categoría de URL)** para ver estadísticas para el usuario o grupo seleccionado.

Ver el informe de actividad del usuario (PAN-OS y Panorama)

STEP 1 | Configure un informe de actividad del usuario

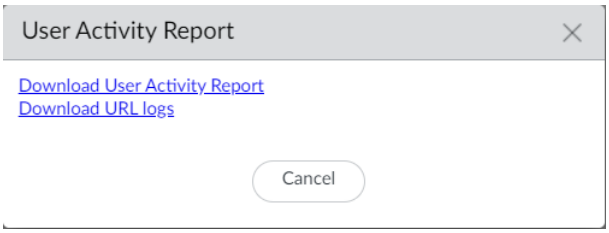
1. Seleccione **Monitor (Supervisar)** > **PDF Reports (Informes en PDF)** > **User Activity Report (Informe de actividad del usuario)**.
2. Haga clic en **Add (Añadir)** para añadir un informe e introduzca un nombre para él en **Name (Nombre)**.
3. Seleccione el **Type (Tipo)** de servidor:
   - Seleccione **User (Usuario)** para generar un informe para una persona.
   - Seleccione **Group (Grupo)** para seleccionar un grupo de usuarios.

   *Debe habilitar el User-ID para poder seleccionar nombres de usuarios o grupos. Si User-ID no se ha configurado, puede seleccionar el tipo **User (Usuario)** e introducir la dirección IP del equipo del usuario.*
4. Introduzca el **Username/IP Address (Nombre de usuario/dirección IP)** de un informe de usuario o introduzca el nombre de grupo de un informe de grupo de usuarios.
5. Seleccione el periodo de tiempo. Puede seleccionar un período de tiempo existente o seleccionar **Custom (Personalizado)**.
6. Seleccione la casilla de verificación **Include Detailed Browsing (Incluir exploración detallada)** para que se incluya información de exploración en el informe.



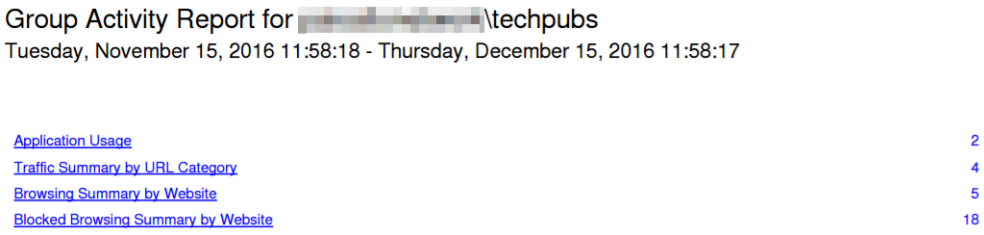
STEP 2 | Ejecute el informe.

1. Haga clic en **Run now (Ejecutar ahora)**.
2. Cuando el cortafuegos termine de generar el informe, haga clic en uno de los enlaces para descargarlo:
   - Haga clic en **Download User Activity Report (Descargar informe de actividad del usuario)** para descargar una versión en PDF del informe.
   - Haga clic en **Download URL Logs (Descargar logs de URL)** para descargar un archivo CSV de las entradas de log correspondientes.

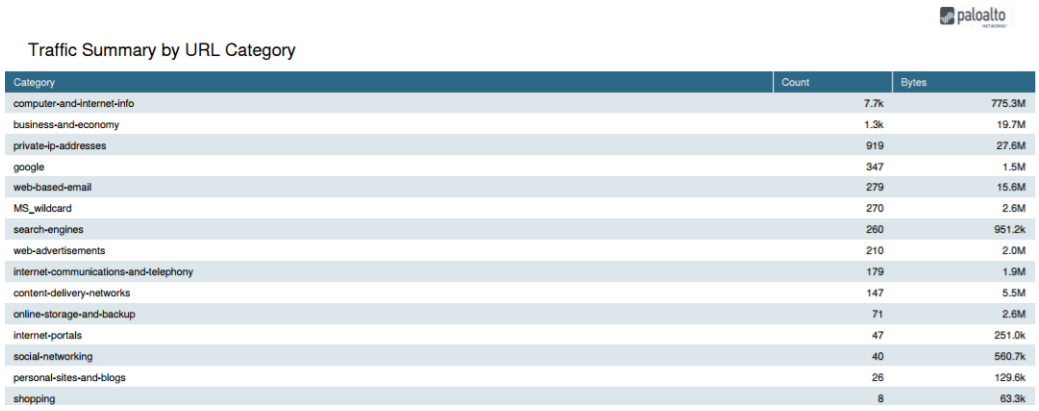


3. Tras descargar el informe, haga clic en **Cancel (Cancelar)**.
4. Si desea guardar la configuración del informe de actividad del usuario para ejecutar el mismo informe nuevamente más tarde, haga clic en **OK (Aceptar)**; de lo contrario, haga clic en **Cancel (Cancelar)**.

STEP 3 | Vea el informe de actividad del usuario abriendo el archivo que descargó. La versión PDF del informe muestra el usuario o el grupo en el que basó el informe, el período de tiempo del informe y un índice:


Group Activity Report for [redacted]\techpubs
Tuesday, November 15, 2016 11:58:18 - Thursday, December 15, 2016 11:58:17

STEP 4 | Haga clic en un elemento del índice para ver los detalles del informe. Por ejemplo, haga clic en **Traffic Summary by URL Category (Resumen de tráfico por categoría de URL)** para ver estadísticas para el usuario o grupo seleccionado.


paloalto

Traffic Summary by URL Category

Category	Count	Bytes
computer-and-internet-info	7.7k	775.3M
business-and-economy	1.3k	19.7M
private-ip-addresses	919	27.6M
google	347	1.5M
web-based-email	279	15.6M
MS_wildcard	270	2.6M
search-engines	260	951.2k
web-advertisements	210	2.0M
internet-communications-and-telephony	179	1.9M
content-delivery-networks	147	5.5M
online-storage-and-backup	71	2.6M
internet-portals	47	251.0k
social-networking	40	560.7k
personal-sites-and-blogs	26	129.6k
shopping	8	63.3k

Programar y compartir informes de URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

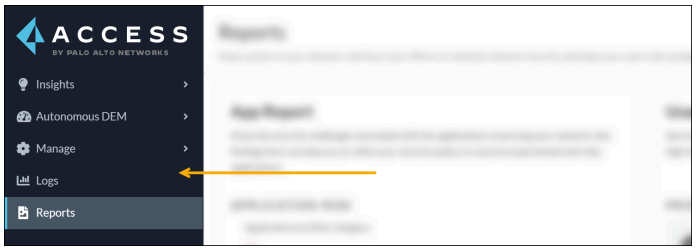
Puede programar, generar y compartir varios informes relacionados con el filtrado de URL y la actividad web.

- Strata Cloud Manager
- PAN-OS y Panorama

Programar y compartir informes de filtrado de URL (Strata Cloud Manager)

Ya sea que esté utilizando Panorama o Strata Cloud Manager para gestionar Prisma Access, puede utilizar Strata Cloud Manager para los informes de filtrado de URL. En Strata Cloud Manager, vaya a Actividad para obtener datos e informes interactivos de filtrado de URL. Puede compartir informes de actividad dentro de su organización y también programarlos para que se actualicen periódicamente. Aquí están los paneles y herramientas de Prisma Access más relevantes y que el filtrado de URL puede aprovechar:

- **Resumen ejecutivo** : vea qué categorías de URL representan la mayor parte de la actividad web en su red, las 10 principales URL maliciosas y las 10 principales URL de alto riesgo.
- **Actividad del usuario**: vea los patrones de navegación de los usuarios individuales: los sitios que visitan con más frecuencia, los sitios con los que transfieren datos y los intentos de acceder a sitios de alto riesgo. Los datos de los logs de Filtrado de URL y Motor de identidad en la nube permiten esta visibilidad.
- Buscar un artefacto de seguridad (una dirección IP, un dominio, una URL o un hash de archivo) para interactuar con los datos solo para ese artefacto, extraídos de los hallazgos de su red y la inteligencia de amenazas global.



Para acceder a los datos de actividad de los usuarios y compartir informes de forma fácil y segura, recomendamos activar *y* configurar el Motor de identidad en la nube.

STEP 1 | Descargar, compartir y programar informes de actividad.

STEP 2 | Acceda al resumen ejecutivo de filtrado de URL.

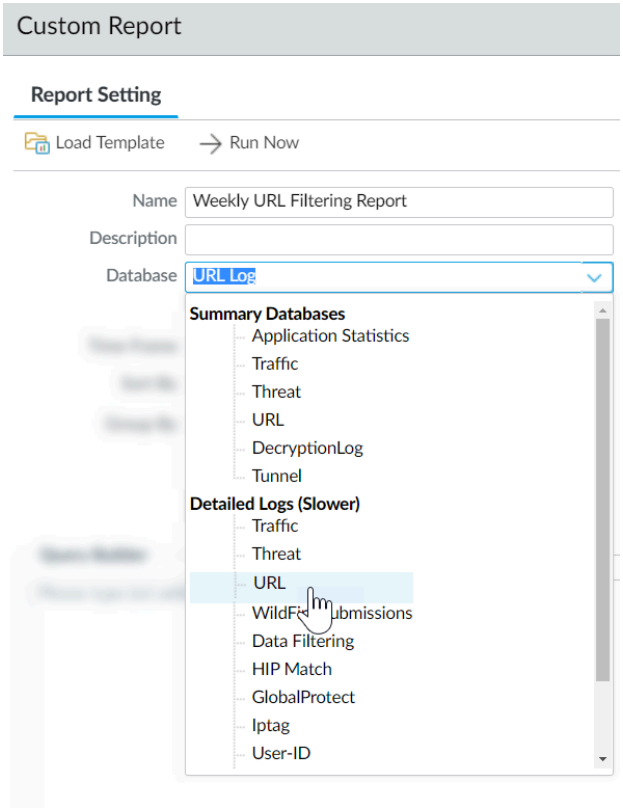
Seleccione **Activity (Actividad)** > **Executive Summary (Resumen ejecutivo)** y haga clic en la pestaña URL Filtering.

STEP 3 | Búsqueda de artefactos de seguridad.

Programar y compartir informes de filtrado de URL (PAN-OS y Panorama)

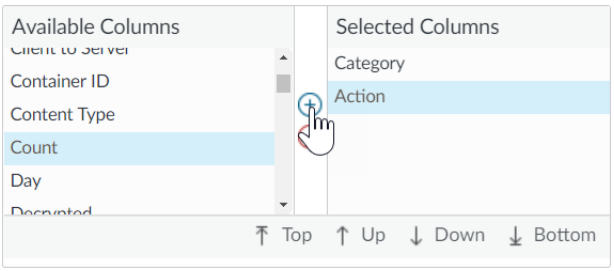
STEP 1 | Añada un nuevo informe personalizado.

1. Seleccione **Monitor (Supervisar)** > **Manage Custom Reports (Gestionar informes personalizados)** y **Add (Añadir)** para añadir un informe.
2. Asigne al informe un **Name (Nombre)** único y, opcionalmente, una **Description (Descripción)**.
3. Seleccione la **Database (Base de datos)** que desea utilizar para generar el informe. Para generar un informe detallado con filtrado de URL, seleccione **URL** de la sección Detailed Logs (Logs detallados):

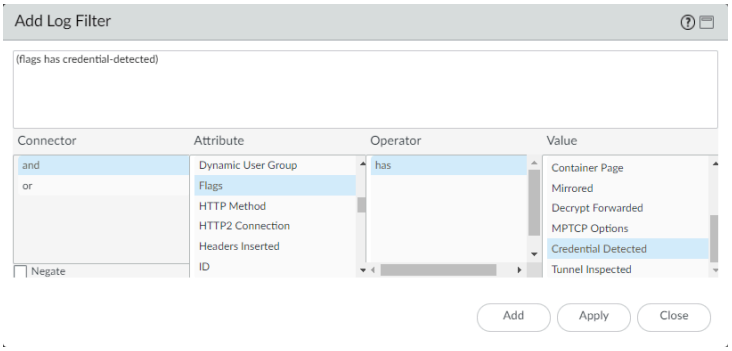


STEP 2 | Configure las opciones de informe.

1. Seleccione un **Time Frame (Período de tiempo)** predefinido o seleccione **Custom (Personalizado)**.
2. Seleccione las columnas de logs que desea incluir en el informe de la lista de columnas disponibles y añádalas ( ) a las columnas seleccionadas. Por ejemplo, para un informe de filtrado de URL, puede seleccionar las siguientes opciones:
   - Acción
   - Categoría de aplicación
   - Category
   - País de destino
   - Source User (Usuario de origen)
   - URL

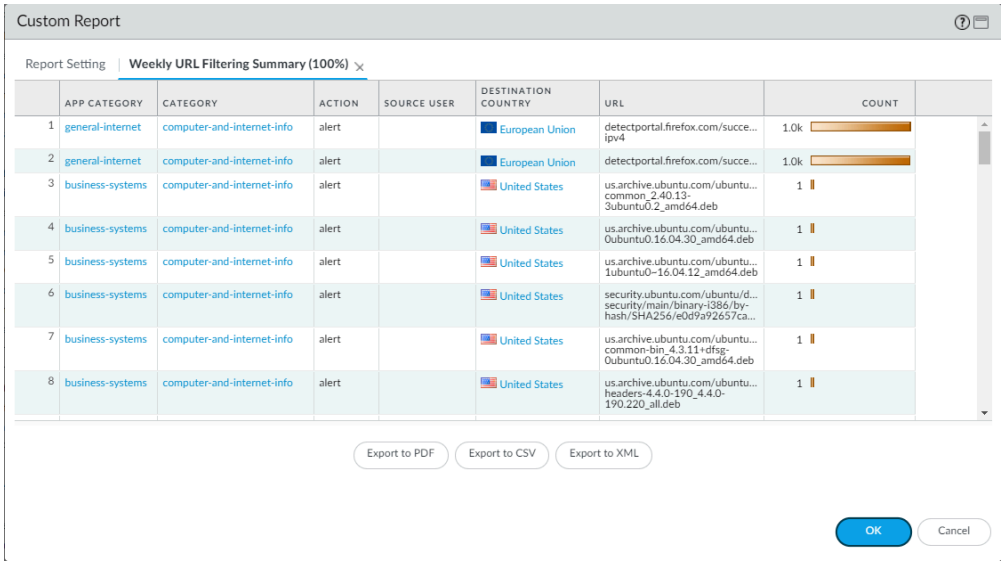


3. Si en el cortafuegos, está habilitada la Prevención de phishing de credenciales, seleccione el atributo **Flags (Marcas)**, el operador **has** y el valor **Credential Detected (Credencial detectada)** para que también se incluyan eventos en el informe que registren cuando un usuario envíe una credencial corporativa válida a un sitio.



4. (Opcional) Seleccione una opción **Sort By (Ordenar por)** para configurar el atributo que se utilizará para agregar los detalles del informe. Si no selecciona un atributo según el cual ordenar, el informe devolverá el primer número N de resultados sin ninguna agregación. Seleccione un atributo **Group By (Agrupar por)** que se utilizará como delimitador para agrupar los datos. El siguiente ejemplo muestra un informe con **Group**

By (Agrupar por) la **App Category (Categoría de aplicaciones)** y **Sort By (Ordenar por)** el **Count (Conteo)** de los **Top 5 (5 principales)**.



STEP 3 | Ejecute el informe.

1. Haga clic en el icono **Run Now (Ejecutar ahora)** para generar inmediatamente el informe que aparecerá en una nueva pestaña.
2. Cuando complete la revisión del informe, vuelva a la pestaña **Report Setting (Configuración de informes)** y modifique la configuración antes de volver a ejecutar el informe, o continúe al próximo paso para programar un informe.
3. Seleccione la casilla de verificación **Schedule (Programación)** para ejecutar el informe una vez al día. Esto generará un informe diario con información detallada de la actividad web las últimas 24 horas.

STEP 4 | Haga clic en **Commit (Confirmar)** para confirmar la configuración.

STEP 5 | Vea el informe personalizado.

1. Seleccione **Monitor (Supervisar)** > **Reports (Informes)**.
2. Expanda el panel **Custom Reports (Informes personalizados)** en la columna derecha y seleccione el informe que desea ver. El informe más reciente se muestra automáticamente.
3. Para ver el informe de una fecha anterior, seleccione la fecha del calendario. También puede exportar el informe a PDF, CSV o XML.

Registro solo de las páginas que visita un usuario

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

Una página contenedora es la página principal a la que accede un usuario al visitar un sitio web, pero se pueden cargar páginas adicionales dentro de la página principal. Si la opción **Log Container page only (Solo página de contenedor de logs)** está habilitada en un perfil de filtrado de URL (perfil de gestión de acceso a URL para Prisma Access), solo se registrará la página principal del contenedor, no las páginas posteriores que puedan cargarse dentro de la página del contenedor. Dado que el filtrado de URL potencialmente puede generar muchas entradas de log, puede que quiera activar esta opción; de este modo, las entradas de log solamente incluirán esos URI cuando el nombre de archivo de la página solicitada coincida con los tipos MIME específicos. El conjunto predeterminado incluye los siguientes tipos MIME:

- application/pdf
- application/soap+xml
- application/xhtml+xml
- text/html
- text/plain
- text/xml

*Si ha habilitado la opción **Log container page only (Solo página de contenedor de logs)**, puede que no siempre haya una entrada de log de URL correlacionada para amenazas detectadas por antivirus o protección frente a vulnerabilidades.*

- Strata Cloud Manager
- PAN-OS y Panorama

Registrar solo las páginas que visita un usuario (Strata Cloud Manager)

Si está utilizando Panorama para gestionar Prisma Access:

*Desplácese a la pestaña **PAN-OS y Panorama** y siga las instrucciones que se indican allí.*

Si usa Strata Cloud Manager, continúe aquí.

STEP 1 | En un perfil de administración de acceso a URL, seleccione **Log Container Page Only (Solo página de contenedor de logs)**.

STEP 2 | Aplique el perfil de Gestión de acceso URL a una regla de la política de seguridad.

Un perfil de gestión de acceso URL solo está activo cuando se incluye en un grupo de perfiles al que hace referencia una regla de la política de seguridad.

Siga los pasos para activar un perfil de gestión de acceso URL (y cualquier perfil de seguridad). No olvide **Push Config (Enviar configuración)**.

Registrar solo las páginas que visita un usuario (PAN-OS y Panorama)

STEP 1 | Cree o seleccione un perfil de filtrado de URL para modificar.

Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **> URL Filtering (Filtrado de URL)**.

STEP 2 | Habilite **Log container page only (Solo página de contenedor de log)**.

STEP 3 | Haga clic en **OK (Aceptar)** para guardar el perfil.

STEP 4 | Haga clic en **Commit (Confirmar)** para compilar los cambios.

Creación de logs del encabezado HTTP

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias dePrisma Access incluyen capacidades de Advanced URL Filtering.*

El filtrado de URL proporciona visibilidad y control sobre el tráfico web de su red. Para aumentar la visibilidad en el contenido web, puede configurar el perfil de filtrado de URL para registrar un log de atributos de encabezado HTTP incluido en una solicitud web. Cuando un cliente solicita una página web, el encabezado HTTP incluye los campos de agente de usuario, sitio de referencia y x-forwarded-for como pares de atributo y valor, y los reenvía al servidor web. En caso de estar habilitado para la creación de logs de encabezados HTTP, el cortafuegos registra los siguientes pares de atributo y valor en los logs de filtrado de URL.

También puede usar encabezados HTTP para gestionar el acceso a las aplicaciones SaaS. No necesita una licencia de filtrado de URL para realizar este procedimiento, pero debe usar un perfil de filtrado de URL para activar esta función.

Atributo	Description (Descripción)
User-Agent (Agente de usuario)	Explorador web que usa el usuario para acceder a la dirección URL (por ejemplo, Internet Explorer). Esta información se envía en la solicitud de HTTP al servidor. El encabezado HTTP no contiene la cadena completa para el Agente de usuario. Los bytes máximos registrados del paquete que precede al paquete que contiene el extremo del encabezado es de 36 bytes.
Referer (Sitio de referencia)	Dirección URL de la página web que dirige al usuario a otra página web. Se trata del origen que redirige (remite) al usuario a la página web que se está solicitando.
X-Forwarded-For (XFF)	Opción del campo de encabezado de solicitud HTTP que conserva la dirección IP del usuario que ha solicitado la página web. Si tiene un servidor proxy en la red, el XFF le permite identificar la dirección IP del usuario que solicitó el contenido,

Atributo	Description (Descripción)
	en lugar de solo registrar la dirección IP del servidor proxy como dirección IP de origen que solicitó la página web.
Headers Inserted (Encabezados insertados)	El tipo de encabezado y el texto del encabezado que inserta el cortafuegos.

Solicitud para cambiar la categoría de una URL

¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Notas:*** • *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.* • *Las licencias de*Prisma Access *incluyen capacidades de Advanced URL Filtering.*

Si cree que un dominio o URL se ha clasificado incorrectamente, puede enviar una solicitud de recategorización a través de su cortafuegos o Test A Site, nuestra herramienta de búsqueda de categorías de URL. También puede enviar solicitudes de recategorización masiva a través de Test A Site. Ambos métodos requieren que sugiera al menos una nueva categoría para la URL que desea revisar.

No es posible solicitar el cambio de la categoría de riesgo *que recibe una URL, ni las URL clasificadas como* `contenido insuficiente` *o* `dominios recién registrados`.

En el cortafuegos, puede solicitar un cambio de categoría de URL desde la vista detallada del log de una entrada de log de filtrado de URL. En Test A Site, debe introducir el sitio web que desea volver a clasificar para ver su categorización PAN-DB. El enlace del formulario de solicitud sigue los resultados de búsqueda. Del mismo modo, en Strata Cloud Manager, se muestra un enlace al formulario de Test A Site con los resultados de las consultas a la herramienta interna Test A Site disponible al editar perfiles de Gestión de acceso URL. Para acceder al formulario de solicitud de cambio masivo, deberá iniciar sesión a Test A Site. Después de iniciar sesión, la página web muestra un enlace al formulario de solicitud masiva.

Inmediatamente después de que alguien envía una solicitud de cambio, un rastreador automatizado analiza la URL. Si el rastreador valida su sugerencia de categoría, Palo Alto Networks aprueba su solicitud y actualiza inmediatamente PAN-DB con la nueva categoría. De lo contrario, los editores humanos de los equipos de investigación de amenazas y ciencia de datos de Palo Alto Networks revisan su solicitud. Pueden decidir mantener la categoría original, estar de acuerdo con la categoría sugerida o cambiar la categoría (si no están de acuerdo con la categoría original y la sugerida).

Después de enviar una solicitud de cambio, recibirá una confirmación por correo electrónico. Una vez que se complete la investigación, recibirá un segundo correo electrónico con los resultados.

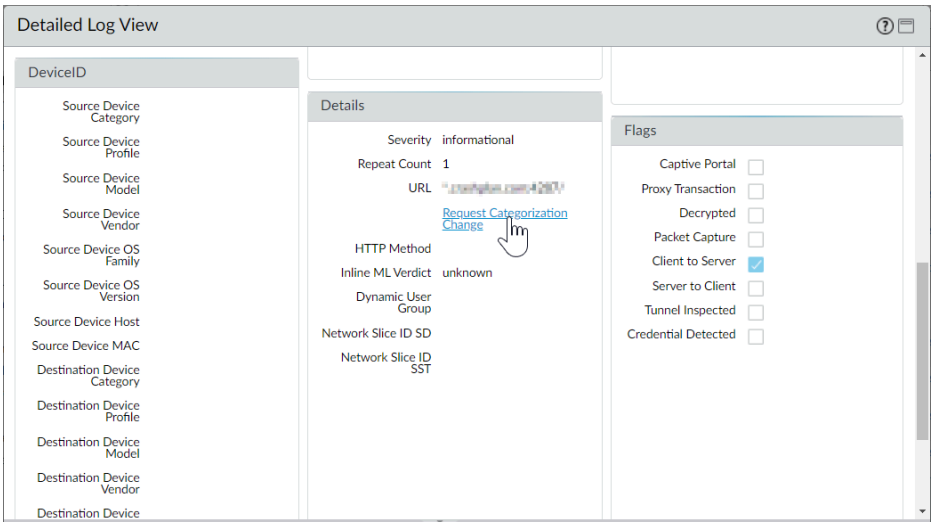
- PAN-OS y Panorama
- Test A Site

Solicitud para cambiar la categoría de una URL (PAN-OS y Panorama)

STEP 1 | Acceda a los logs de Filtrado de URL [**Monitor (Supervisar)** > **Logs** > **URL Filtering (Filtrado de URL)**].

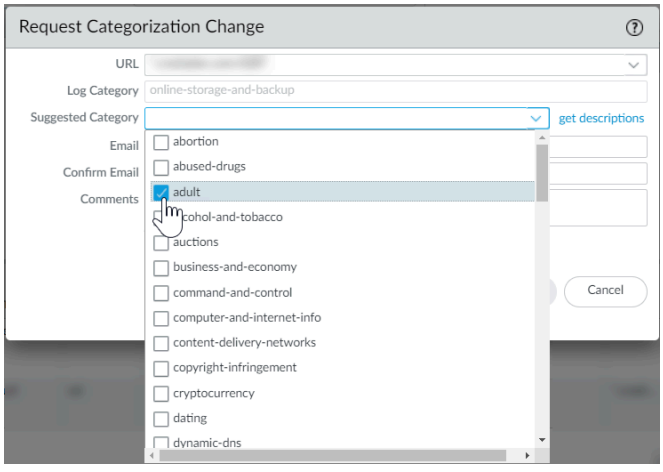
STEP 2 | Abra la vista detallada del log para una entrada de log de filtrado de URL con la categorización de URL que desea cambiar.

1. Haga clic en el catalejo ( ) que corresponde a la entrada del log. Aparece la vista detallada del log.



STEP 3 | En Detalles, haga clic en **Request Categorization Change (Solicitar cambio de categorización)**.

STEP 4 | Complete el formulario de solicitud y envíelo.



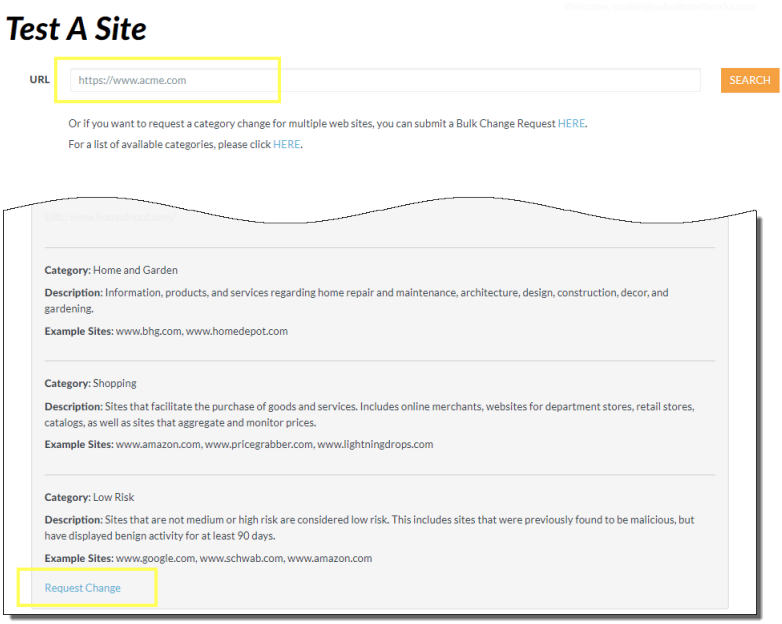
Solicitud para cambiar la categoría de una URL (Test A Site)

STEP 1 | Diríjase a Test A Site.

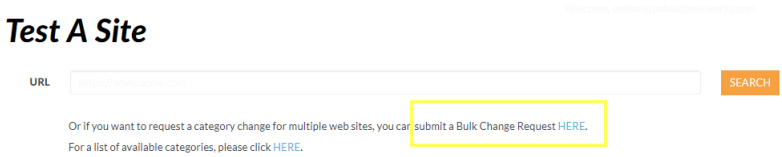
> ***Log in (Inicie sesión)*** *para evitar completar una prueba CAPTCHA y para introducir su correo electrónico en el formulario de solicitud de cambio. Tenga en cuenta que iniciar sesión es la única manera de acceder al formulario de solicitud de cambio masivo.*

STEP 2 | Seleccione un formulario de solicitud de cambio para completar.

- **Solicitud de cambio para una única URL**: introduzca la **URL** que desea volver a clasificar y haga clic en **Search (Buscar)**. Debajo de los resultados de la categoría de URL, haga clic en **Request Change (Solicitar cambio)**.



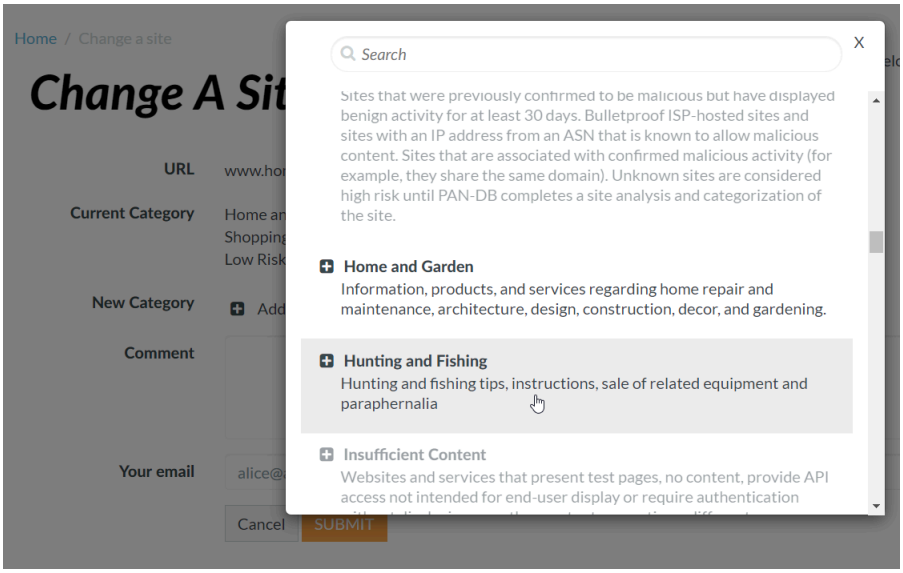
- **Solicitud de cambio masivo**: **Log in (Inicie sesión)** en Test A Site. Luego, haga clic en enviar una solicitud de cambio masivo **HERE (Aquí)**.



STEP 3 | Complete el formulario de solicitud de cambio.

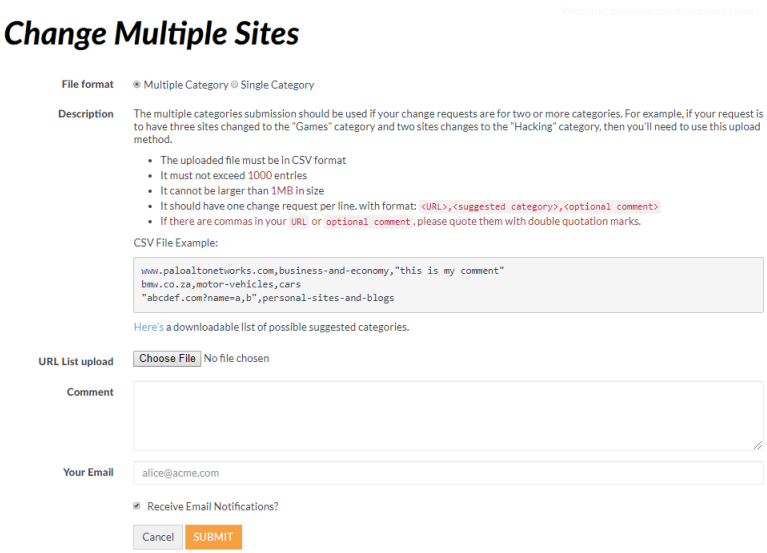
- **Solicitud de cambio para una única URL**: sugiera hasta dos categorías nuevas para la URL. Haga clic en **Select category (from a list) [Seleccionar categoría (de una lista)]** y seleccione

una categoría a la vez. Opcionalmente, deje un **Comment (Comentario)** sobre su solicitud. Puede explicar por qué su sugerencia es apropiada, por ejemplo.



- **Solicitud de cambio masivo**: seleccione un **File Format (Formato de archivo)**. Seleccione Múltiples categorías si su solicitud de cambio incluye dos o más categorías. Por ejemplo, si quiere volver a clasificar la mitad de las URL de su lista a `empresas y economía` y la otra mitad a `sitios personales y blogs`.

  Luego, haga clic en **Choose File (Elegir archivo)** y seleccione un archivo CSV para cargar. El archivo debe tener una solicitud de cambio por línea en este formato: <URL>,`<first suggested category>,<second suggested category>,<(optional) comment>`. El archivo no puede superar 1000 entradas o ser superior a 1 MB. Opcionalmente, deje un **Comment (Comentario)** sobre su solicitud.



STEP 4 | **Submit (Enviar)** el formulario.

Resolución de problemas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

En este capítulo se comparten las tareas para diagnosticar y resolver problemas comunes de filtrado de URL para los cortafuegos de nueva generación de Palo Alto Networks. Antes de ponerse en contacto con la asistencia técnica de Palo Alto Networks con respecto a estos problemas, complete los pasos de las tareas correspondientes. Si aún necesita ponerse en contacto con la asistencia técnica, asegúrese de incluir toda la información que obtuvo al realizar tareas de resolución de problemas.

La solución de problemas y la supervisión de la actividad web suelen ir de la mano. Aproveche las herramientas de supervisión y creación de logs con frecuencia para identificar y solucionar problemas que no se tratan explícitamente en este capítulo. Familiarícese con las herramientas y tareas de supervisión en el capítulo de Supervisión.

- Problemas al activar Advanced URL Filtering
- Problemas de conectividad con la nube de PAN-DB
- URL clasificadas como no resueltas
- Categorización incorrecta
- Resolución de problemas de acceso al sitio web
- Resolución de problemas de visualización de la página de respuesta del filtrado de URL

Problemas al activar Advanced URL Filtering

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Utilice el siguiente flujo de trabajo para solucionar problemas de activación del Advanced URL Filtering.

STEP 1 | Acceda a la CLI de PAN-OS.

STEP 2 | Compruebe si se ha activado Advanced URL Filtering ejecutando el siguiente comando:

```
show system setting url-database
```

Si la respuesta es `paloaltonetworks`, PAN-DB, la base de datos de filtrado de URL de Palo Alto Networks, es el proveedor activo.

STEP 3 | Compruebe que el cortafuegos tiene una licencia de Advanced URL Filtering válida.

Ejecute el comando de la CLI **`request license info`**.

Debería de ver la entrada de licencia `Feature (Función): Advanced URL Filtering`. Si la licencia no está instalada, deberá obtener e instalar una. Consulte Configuración de URL Filtering.

STEP 4 | Compruebe el estado de la conexión en la nube de PAN-DB.

Problemas de conectividad con la nube de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Para ayudar a garantizar la conectividad a la nube PAN-DB, cree una regla de política de seguridad dedicada que permita todo el tráfico del servicio de gestión de Palo Alto. Esto evitará que el tráfico de gestión se clasifique como `no resuelto` *y evitará que el tráfico se bloquee cuando se enruta a través del plano de datos.*

Para verificar la conectividad entre el cortafuegos y la nube PAN-DB:

```
show url-cloud status
```

Si se puede acceder a la nube, la respuesta esperada es similar a la siguiente:

```
show url-cloud status PAN-DB URL Filtering License : valid
 Current cloud server : serverlist.urlcloud.paloaltonetworks.com
 Cloud connection : connected Cloud mode : public URL database
 version - device : 20200624.20296 URL database version - cloud :
 20200624.20296 ( last update time 2020/06/24 12:39:19 ) URL
 database status : good URL protocol version - device : pan/2.0.0 URL
 protocol version - cloud : pan/2.0.0 Protocol compatibility status :
 compatible
```

Si no se puede acceder a la nube, la respuesta esperada es similar a la siguiente:

```
show url-cloud status PAN-DB URL Filtering License : valid Cloud
 connection : not connected URL database version - device :
 0000.00.00.000 URL protocol version - device : pan/0.0.2
```

Utilice la siguiente lista de verificación para identificar y resolver problemas de conectividad:

- ❑ ¿Se muestra el campo de licencia de filtrado de URL de PAN-DB como no válido? Obtenga e instale una licencia válida de PAN-DB.
- ❑ ¿Se muestra la versión del protocolo de URL como no compatible? Actualice PAN-OS a la versión más reciente.

- ¿Puede enviar un ping al servidor de nube de PAN-DB desde el cortafuegos? Ejecute el siguiente comando para comprobarlo:

  ```
  ping source <ip-address> host
   serverlist.urlcloud.paloaltonetworks.com <
  ```

  Por ejemplo, si la dirección IP de su interfaz de gestión es 10.1.1.5, ejecute el siguiente comando:

  ```
  ping source 10.1.1.5 host serverlist.urlcloud.paloaltonetworks.com
  ```

- ¿Se encuentra el cortafuegos en una configuración de HA? Compruebe que el estado de HA de los cortafuegos se encuentre en un estado activo, activo-principal o activo-secundario. El acceso a la nube de PAN-DB se bloqueará si el cortafuegos tiene un estado diferente: Ejecute el siguiente comando en cada cortafuegos del par para observar el estado:

  ```
  show high-availability state
  ```

Si aún tiene problemas de conectividad entre el cortafuegos y la nube de PAN-DB, póngase en contacto con el equipo de asistencia técnica de Palo Alto Networks.

URL clasificadas como no resueltas

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Las URL se clasifican como `no resueltas` si su cortafuegos no puede conectarse al servicio en la nube del filtrado de URL de PAN-DB para realizar búsquedas, o si PAN-DB tarda demasiado en responder a las consultas de URL. El estado de la conexión a la nube y la clasificación de URL no se aplican a las licencias de suscripción caducadas ni a los usuarios sin licencia. Para obtener una explicación detallada del proceso de categorización de URL, consulte Cómo funciona el filtrado de URL.

Utilice el siguiente flujo de trabajo para solucionar problemas en los que algunas o todas las URL identificadas por PAN-DB se clasifican como no resueltas:

STEP 1 | Compruebe la conexión en la nube PAN-DB ejecutando el comando de la CLI **`show url-cloud status`**.

En el campo de `Conexión con la nube` se deberá mostrar `Conectado`. Si no se muestra `conectado`, entonces cualquier URL que no exista en la caché del plano de gestión se categoriza como `no resuelto`. Para solucionar este problema, consulte Problemas de conectividad con la nube de PAN-DB.

STEP 2 | Si el estado de conexión de la nube es `Conectado`, compruebe el uso actual del cortafuegos.

Si el rendimiento del cortafuegos tiene picos, puede que las solicitudes de URL se descarten (puede que no lleguen al plano de gestión) y se clasifiquen como `not-resolved`.

Para ver los recursos del sistema, ejecute el comando de la CLI **`show system resources`**. Luego, vea las columnas `%CPU` y `%MEM`.

También puede ver los recursos del sistema en el widget System Resouces (Recursos del sistema) en el **Dashboard (Panel)** en la interfaz web.

STEP 3 | Considere aumentar el valor del **Category lookup timeout (sec) [Tiempo de espera de búsqueda de categoría (seg)]**.

Aumentar el valor de tiempo de espera de búsqueda de categoría mejora la probabilidad de que la categoría de URL se resuelva y reduce la frecuencia de URL `no resueltas` en los logs.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** y edite la configuración de filtrado de URL.
2. Haga clic en **OK (Aceptar)** y en **Commit (Confirmar)** para aplicar los cambios.

   También puede actualizar el valor mediante el comando de la CLI **`set deviceconfig setting ctd url-wait-timeout`**.

STEP 4 | Si el problema persiste, póngase en contacto con el soporte técnico de Palo Alto Networks.

Categorización incorrecta

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Es posible que, a veces, considere que algunas URL están categorizadas incorrectamente. Utilice el siguiente flujo de trabajo para determinar la categorización de una URL para un sitio y solicitar un cambio de categoría, de ser necesario.

STEP 1 | Compruebe la categoría en el plano de datos mediante la ejecución del siguiente comando:

```
show running url <URL>
```

Por ejemplo, para ver la categoría del sitio web de Palo Alto Networks, ejecute el siguiente comando:

```
show running url paloaltonetworks.com
```

Si la URL almacenada en la caché del plano de datos tiene la categoría correcta (información de equipo e internet en este ejemplo), la categorización es correcta y no es necesario realizar ninguna otra acción. Si la categoría no es correcta, vaya al paso siguiente.

STEP 2 | Compruebe la categoría en el plano de gestión mediante la ejecución del siguiente comando:

```
test url-info-host <URL>
```

Por ejemplo:

```
test url-info-host paloaltonetworks.com
```

Si la URL almacenada en la caché del plano de gestión tiene la categoría correcta, quite la URL de la caché del plano de datos mediante la ejecución del siguiente comando:

```
clear url-cache url <URL>
```

La próxima vez que el cortafuegos solicite la categoría de esta URL, la solicitud se reenviará al plano de gestión. Esto solucionará el problema y no será necesario realizar ninguna otra acción. Si esto no soluciona el problema, vaya al paso siguiente para comprobar la categoría de URL en los sistemas de la nube.

STEP 3 | Compruebe la categoría en la nube mediante la ejecución del siguiente comando:

```
test url-info-cloud <URL>
```

STEP 4 | Si la URL almacenada en la nube tiene la categoría correcta, quite la URL de las cachés del plano de datos y el plano de gestión.

Ejecute el siguiente comando para eliminar una URL de la caché del plano de datos:

```
clear url-cache url <URL>
```

Ejecute el siguiente comando para eliminar una URL de la caché del plano de gestión:

```
delete url-database url <URL>
```

La próxima vez que el cortafuegos solicite la categoría de la URL dada, la solicitud se reenviará al plano de gestión y, a continuación, a la nube. Esto debería solucionar el problema de búsqueda de categoría. Si el problema persiste, consulte el paso siguiente para enviar una solicitud de cambio de categorización.

STEP 5 | Para enviar una solicitud de cambio desde la interfaz web, vaya al log de URL y seleccione la entrada de log para la URL que desee cambiar.

STEP 6 | Haga clic en el enlace **Request Categorization (Solicitar cambio de categorización)** y siga las instrucciones. Además, para solicitar un cambio de categoría en el sitio web Test A Site de Palo Alto Networks, busque la URL y, a continuación, haga clic en el icono **Request Change (Solicitar cambio)**. Para ver las descripciones de cada categoría, consulte Categorías URL predefinidas.

Si la solicitud de cambio se aprueba, recibirá una notificación por correo electrónico. A continuación, tiene dos opciones para asegurarse de que la categoría de URL se actualiza en el cortafuegos:

- Espere hasta que la URL de la caché caduque y la próxima vez que un usuario acceda a la URL, la actualización de la nueva categorización se incluirá en la caché.
- Ejecute el siguiente comando para forzar la actualización en la caché:

```
request url-filtering update url <URL>
```


Resolución de problemas de acceso al sitio web

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Los usuarios finales pueden tener problemas para acceder a un sitio web por varios motivos, como la falta de una licencia de filtrado de URL, una configuración incorrecta de la regla de la política, problemas de conectividad PAN-DB o una categorización incorrecta de un sitio web. Siga estos pasos para diagnosticar y resolver problemas con el acceso a un sitio web.

Es posible que el problema no esté relacionado con el filtrado de URL. La sección "Qué hacer a continuación", que sigue a los pasos de esta tarea, se enumeran áreas adicionales en las que centrar la resolución de problemas.

STEP 1 | Compruebe que tiene una licencia activa de Advanced URL Filtering o de filtrado de URL heredada.

Se necesita una licencia de filtrado de URL activa para que los cortafuegos de nueva generación clasifiquen con precisión los sitios web y las aplicaciones. Si no tiene una licencia de filtrado de URL, el problema de acceso al sitio web no está relacionado con el filtrado de URL.

Seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y busque la licencia de Advanced URL Filtering (o filtrado de URL PAN-DB). Una licencia activa muestra una fecha de caducidad posterior a la fecha actual.

Como alternativa, utilice el comando de la CLI **`request license info`**. Si la licencia está activa, la interfaz muestra la información de la licencia, incluido el estado de caducidad: `¿Caducado?: no`

STEP 2 | Verificar el estado de la conexión a la nube PAN-DB en la CLI.

En el campo de `Conexión con la nube` se deberá mostrar `Conectado`. De lo contrario, cualquier dirección URL que no exista en la caché del plano de gestión (MP) se clasificará como `no resuelta` y puede estar bloqueada por la configuración del perfil de URL Filtering en las reglas de la política de seguridad.

STEP 3 | Borre la caché de MP y plano de datos (DP) de la URL específica.

Borrar la caché puede consumir muchos recursos. Considere la posibilidad de borrar la memoria caché durante un período de mantenimiento.

1. Para borrar la caché de MP, use el comando de la CLI **`delete url-database url <url afectada>`**.
2. Para borrar la caché de DP, use el comando de la CLI **`clear url-cache url < url afectada>`**.

STEP 4 | Revise los logs de filtrado de URL para verificar si se ha bloqueado la categoría de URL a la que pertenece el sitio web.

1. Seleccione **Monitor (Supervisar)** > **URL Filtering (Filtrado de URL)**.
2. Busque la dirección URL afectada y, a continuación, seleccione la entrada de log más reciente.
3. Revise las columnas Categoría y Acción.

   ¿Se ha clasificado correctamente la URL? Verifique sus categorías usando Test A Site, herramienta de búsqueda de categorías de URL de Palo Alto Networks. Si sigue creyendo que la categorización es incorrecta, envíe una solicitud de cambio.

   Si se muestra la columna Acción `block-url`, entonces, anote el nombre de la regla de la política de seguridad asociada a la entrada de log.

STEP 5 | Revise la regla de la política de seguridad y actualícela, si es necesario.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**y seleccione la regla de política con el nombre que anotó en el paso anterior.
2. Compruebe que la regla de la política de seguridad permite el acceso a la URL solicitada o a su categoría de URL.

   Busque una de estas dos configuraciones:

   - **Categoría de URL como criterio de coincidencia:** En **Service/URL Category (Categoría de servicio/URL)**, una de las categorías especificadas contiene la URL solicitada. En **Actions (Acciones)**, la configuración de acción está definida como **Allow (Permitir)**.
   - **Perfil de URL Filtering:** En **Actions (Acciones)**, la configuración del perfil se establece en un perfil de filtrado de URL que permite el acceso a la URL solicitada.

STEP 6 | Pruebe las reglas de la política de seguridad.

Si los pasos anteriores no resaltan o resuelven el problema, es posible que se requiera soluciones adicionales para aislar aún más el problema. Las áreas de enfoque deberán incluir:

- Conectividad básica de direcciones IP
- Configuración de enrutamiento
- Resolución DNS
- Configuración de proxy
- Cortafuegos ascendente o dispositivos de inspección en la ruta del paquete

Para problemas intermitentes o complejos, póngase en contacto con la asistencia de Palo Alto Networks para obtener más ayuda.

Resolución de problemas de visualización de la página de respuesta del filtrado de URL

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Es posible que las páginas de respuesta del filtrado de URL no se muestren por diversos motivos, entre ellos:

- Las inspecciones de protocolo de enlace SSL/TLS están habilitadas.
- El sitio web fue bloqueado durante la inspección de un protocolo de enlace SSL/TLS. Las páginas de respuesta del filtrado de URL no se muestran en este caso porque el cortafuegos restablece la conexión HTTPS.
- El sitio web utiliza el protocolo HTTPS o contiene contenido servido sobre HTTPS (como anuncios), pero el sitio web o la categoría de URL no se descifró.
- La página de respuesta personalizada es más grande que el tamaño máximo admitido.

Utilice los siguientes pasos como punto de partida para solucionar problemas de una página de respuesta de filtrado de URL que no se muestra. Si el problema persiste, póngase en contacto con el soporte técnico de Palo Alto Networks.

STEP 1 | Determine el alcance del problema.

¿El problema es específico de un sitio web en particular o de un subconjunto de páginas web? Compruebe si se muestra una página de respuesta cuando visita una página diferente en el sitio web.

STEP 2 | Identifique el protocolo del sitio web (HTTP o HTTPS).

Esta distinción ayuda a aislar y diagnosticar aún más el problema.

STEP 3 | (Sitios HTTPS o sitios HTTP con contenido HTTPS) Verifique que una regla de la política de descifrado SSL/TLS descifre el tráfico al sitio web o la categoría de URL.

En general, el cortafuegos no puede servir páginas de respuesta en sitios web HTTPS a menos que pueda descifrar dichos sitios web.

Algunos sitios web pueden mostrar su página principal mediante HTTP pero mostrar anuncios u otro contenido mediante HTTPS. Estos sitios web también deben descifrarse para garantizar la visualización de las páginas de respuesta.

1. Inicie sesión en la interfaz web.
2. Seleccione **Policies (Políticas)** > **Decryption (Descifrado)** y verifique que la regla relevante descifre el tráfico al sitio web o categoría de URL específicos.

   Si este no es el caso, actualice la regla de la política de descifrado para descifrar el sitio web o la categoría de URL.

- Si el descifrado SSL/TLS está habilitado y la página de respuesta aún no se muestra, habilite la inspección de los protocolos de enlace SSL/TLS.
- Para servir una página de respuesta de filtrado de URL en una sesión HTTPS sin habilitar el descifrado SSL/TLS, siga estos pasos.

STEP 4 | Verifique que la categoría de URL a la que pertenece el sitio web se ha bloqueado.

Si la categoría se ha bloqueada en un perfil de URL Filtering aplicado a una Regla de la política de seguridad o por una Regla de la política de seguridad con la categoría de URL específica como criterio de coincidencia, el valor en la columna Acción para una entrada determinada muestra `block-url`.

1. Seleccione **Monitor (Supervisar)** > **URL Filtering (Filtrado de URL)**.
2. Busque el sitio web afectado y seleccione la entrada de registro más reciente.
3. Examine las columnas Categoría y Acción.

   ¿Son precisas las categorías asignadas al sitio web? Verifique sus categorías usando Test A Site, herramienta de búsqueda de categorías de URL de Palo Alto Networks. Si aún cree que el sitio web se ha categorizado de forma incorrecta, envíe una solicitud de cambio.

   ¿El valor de Acción es `block-url`? De lo contrario, actualice el perfil de URL Filtering o la regla de la política de seguridad.
4. Para referencia futura, tenga en cuenta la regla asociada con esta entrada de log.

STEP 5 | Determine si una página de respuesta personalizada es la causa de este problema.

1. Seleccione **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)**.
2. Confirme que solo **Predefined (Predefinido)** esté seleccionado.

   Una página de respuesta personalizada está activa si **shared (compartido)** aparece [además de **Predefined (Predefinido)**] en cualquiera de estos lugares:

   - **Device (Dispositivo)** > **Response Pages (Página de respuesta)**: En la columna Ubicación correspondiente a una página de respuesta determinada.
   - **Device (Dispositivo)** > **Response Pages (Páginas de respuesta)** > ***Type (Tipo)***: En Ubicación.
3. (Si **Shared (Compartido)** está incluido en la lista) Revierta la página personalizada a su estado predeterminado para confirmar que la página de respuesta personalizada es el problema.

   1. Seleccione **Delete (Eliminar)** para eliminar la página personalizada.
   2. Haga clic en **Commit (Confirmar)** para compilar los cambios.
   3. Visite el sitio web afectado para ver si se muestra la página de respuesta predeterminada.

   Si el problema persiste, llame a la asistencia técnica para realizar una investigación más exhaustiva.

Si los pasos anteriores no solucionan el problema, póngase en contacto con la asistencia de Palo Alto Networks. Es posible que sea necesario realizar una resolución de problemas adicional para identificar el problema. Por ejemplo, analizar el tráfico a través de una herramienta de captura de paquetes (pcap) junto con soporte puede ser útil si una página de respuesta no funciona para algunas páginas web pero sí para otras.

Nube privada de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

La nube privada de PAN-DB proporciona una solución local para las organizaciones que restringen el uso de los servicios en la nube pública. En particular, los cortafuegos consultan los servidores de nube privada PAN-DB durante las búsquedas de URL en lugar de los servidores de nube pública PAN-DB. Para implementar esta solución, deberá implementar una o varios dispositivos M-600 o M-700 como servidores PAN-DB dentro de su red o centro de datos. Solo los cortafuegos que ejecutan PAN-OS 9.1 o versiones posteriores pueden comunicarse con la nube privada PAN-DB.

Las implementaciones de nube privada de PAN-DB no son compatibles con las funciones de análisis de URL basadas en la nube de la suscripción de Advanced URL Filtering.

En la siguiente tabla se describen las diferencias entre la nube pública de PAN-DB y la nube privada de PAN-DB.

Table 1: Diferencias entre la nube pública de PAN-DB y la nube privada de PAN-DB

Diferencias	Nube pública de PAN-DB	Nube privada de PAN-DB
Actualizaciones de contenido y base de datos	Las actualizaciones de contenido (periódicas y críticas) y las actualizaciones completas de la base de datos de URL se publican varias veces al día. La nube pública de PAN-DB actualiza las categorías de las URL de malware y phishing cada cinco minutos. El cortafuegos también comprueba actualizaciones críticas siempre que consulta a los servidores de nube para búsquedas de URL.	Las actualizaciones de contenido y las actualizaciones de bases de datos de URL completas están disponibles una vez al día durante la semana.
Solicitudes de categorización de URL	Puede solicitar un cambio de categorización de URL a través de: • Sitio web de comprobación de sitios de Palo Alto Networks. • Un perfil de filtrado de URL.	Puede solicitar un cambio de categorización de URL a través del sitio web Test A Site de Palo Alto Networks.

Diferencias	Nube pública de PAN-DB	Nube privada de PAN-DB
	• Un log de filtrado de URL.	
Consultas URL sin resolver	Si el cortafuegos no puede resolver una consulta de URL, la solicitud se envía a los servidores en la nube pública.	Si el cortafuegos no puede resolver una consulta, la solicitud se envía a los dispositivos en la nube privada PAN-DB. Si no hay una coincidencia para la URL, la nube privada de PAN-DB envía un mensaje de respuesta de categoría *desconocida* al cortafuegos; la solicitud no se envía a la nube pública a menos que haya configurado sus dispositivos para acceder a la nube pública de PAN-DB. Si los dispositivos de la nube privada PAN-DB funcionan completamente sin conexión, el cortafuegos no envía ningún dato ni análisis a la nube pública.

- Cómo funciona la nube privada de PAN-DB
- Dispositivos de nube privada de PAN-DB
- Configurar la nube privada de PAN-DB

Cómo funciona la nube privada de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Cuando configure la nube privada de PAN-DB, puede configurar sus dispositivos M-600 o M-700 para tener acceso directo a Internet o permanecer sin conexión. Los dispositivos requieren actualizaciones de la base de datos y contenido para realizar búsquedas de URL. Si los dispositivos no tienen una conexión a Internet activa, debe descargar manualmente las actualizaciones a un servidor de su red e importarlas a cada dispositivo M-600 o M-700 en la nube privada de PAN-DB mediante el SCP. Además, el dispositivo debe poder obtener la base de datos de valores de inicialización y cualquier otra actualización de contenido normal o crítica de los cortafuegos a los que atiende.

El proceso de búsqueda de URL es el mismo para cortafuegos tanto en implementaciones de nube pública como privada. Sin embargo, en implementaciones de nube privada, los cortafuegos consultan a los servidores en la nube privada PAN-DB. Tendrá que especificar la dirección IP o el FQDN de cada servidor M-600 o M-700 que puedan consultar para conceder a sus cortafuegos acceso a los servidores privados en la nube.

Los dispositivos M-600 y M-700 utilizan certificados de servidor preempaquetados para autenticar cortafuegos que se conectan a la nube privada PAN-DB. No puede importar ni usar otro certificado de servidor para autenticar. Si cambia el nombre de host de un dispositivo, el dispositivo genera automáticamente un nuevo conjunto de certificados para autenticar los cortafuegos.

Dispositivos de nube privada de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Para implementar una nube privada de PAN-DB, necesita uno o más dispositivos M-600 o M-700. Ambos dispositivos se entregan en modo Panorama, pero para implementarlos como una nube privada de PAN-DB, debe configurarlos para que funcionen en modo PAN-URL-DB. En el modo PAN-URL-DB, el dispositivo ofrece los servicios de categorización de URL para empresas que no desean usar la nube pública de PAN-DB.

Los dispositivos M-600 y M-700, cuando se implementan como una nube privada de PAN-DB, usan dos puertos: MGT (Eth0) y Eth1; Eth2 no está disponible para su uso. El puerto de gestión se usa para el acceso administrativo al dispositivo y para obtener las últimas actualizaciones de contenido desde la nube pública de PAN-DB o un servidor en su red. Para una comunicación entre la nube privada de PAN-DB y los cortafuegos de la red, puede usar el puerto MGT o Eth1.

El dispositivo M-200 no se puede implementar como una nube privada de PAN-DB.

Los dispositivos M-600 y M-700 en modo PAN-URL-DB:

- No tiene una interfaz web, solo admite una interfaz de línea de comandos (CLI).
- No puede ser gestionado por Panorama.
- No puede implementarse en un clúster en alta disponibilidad (HA).
- No requiere una licencia de filtrado de URL. Los cortafuegos deben tener una licencia de PAN-DB URL Filtering para conectar con la nube privada de PAN-DB y consultarla.
- Se envía con un conjunto de certificados de servidor predeterminados que se usan para autenticar los cortafuegos que se conectan con la nube privada de PAN-DB. No puede importar ni usar otro certificado de servidor para autenticar los cortafuegos. Si cambia el nombre de host de cualquiera de los dispositivo, el dispositivo genera automáticamente un nuevo conjunto de certificados para autenticar los cortafuegos a los que atiende.
- Solo se puede restablecer al modo Panorama. Si desea implementar el dispositivo como recopilador de logs dedicado, cambie al modo Panorama y defínalo en el modo de recopilación de logs.

Configurar la nube privada de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Para implementar uno o más dispositivos M-600 o M-700 como una nube privada de PAN-DB en su red o centro de datos, debe completar las siguientes tareas:

- Configurar la nube privada de PAN-DB
- Configurar cortafuegos para acceder a la nube privada de PAN-DB
- Configuración de la autenticación con certificados personalizados en la nube privada de PAN-DB.

Configuración de la nube privada de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

STEP 1 | Monte en bastidor el dispositivo M-600 o M-700.

Consulte las instrucciones de instalación del bastidor en la guía de referencia de hardwarecorrespondiente.

STEP 2 | Registre el dispositivo.

STEP 3 | Realice la configuración inicial del dispositivo.

Los dispositivos M-600 y M-700, en modo PAN-DB, utilizan dos puertos: MGT (Eth0) y Eth1; Eth2 no se utiliza en modo PAN-DB. El puerto de gestión se usa para el acceso administrativo al dispositivo y para obtener las últimas actualizaciones de contenido desde la nube pública de PAN-DB. Para una comunicación entre el dispositivo (servidor PAN-DB) y los cortafuegos de la red, puede usar el puerto MGT o Eth1.

1. Conéctese al dispositivo de una de las siguientes maneras:
   - Conecte un cable serie desde un ordenador al puerto de la consola del dispositivo y conecte usando un software de emulación de terminal (9600-8-N-1).
   - Conecte un cable Ethernet RJ-45 desde un ordenador hasta el puerto MGT del dispositivo. En un navegador, vaya a https://192.168.1.1. Para habilitar el acceso a esta URL tal vez deba cambiar la dirección IP del ordenador por una dirección de la red 192.168.1.0 (por ejemplo, 192.168.1.2).
2. Cuando se le indique, inicie sesión en el dispositivo. Inicie sesión usando el nombre de usuario y contraseña predeterminados (admin/admin). El dispositivo comenzará a inicializarse.
3. Configure los ajustes de acceso a la red, incluida la dirección IP para la interfaz MGT:

   Utilice el siguiente comando de la CLI: **set deviceconfig system ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***.

   Descripciones de las variables:
   - *<server-IP>* es la dirección IP que desea asignar a la interfaz de gestión del servidor
   - *<netmask>* es la máscara de subred
   - *<gateway-IP>* es la dirección IP de la puerta de enlace de la red, y *<DNS-IP>* es la dirección IP del servidor DNS principal
   - *<DNS-IP>* es la dirección IP del servidor DNS
4. Configure los ajustes de acceso a la red, incluida la dirección IP para la interfaz Eth1:

   Use the following command: **set deviceconfig system eth1 ip-address *<server-IP>* netmask *<netmask>* default-gateway *<gateway-IP>* dns-setting servers primary *<DNS-IP>***.
5. Guarde sus cambios en el servidor PAN-DB.

   Utilice el comando **commit** para confirmar.

STEP 4 | Cambie al modo de nube privada de PAN-DB.

Puede cambiar del modo Panorama al modo PAN-DB y viceversa; y del modo Panorama al modo de recopilador de logs y viceversa. No se permite cambiar directamente desde el modo PAN-DB al modo de recopilador de logs ni viceversa. El cambio de modos operativos activa el restablecimiento de datos. A excepción de la configuración de acceso de gestión, todas las configuraciones y logs existentes se eliminan al reiniciar.

1. Para cambiar al modo PAN-DB, utilice el comando **`request system system-mode pan-url-db`** .
2. Para verificar el cambio de modo, utilice el comando **`show system info`**.

   Si ha cambiado correctamente al modo de nube privada de PAN-DB, el campo `system-mode` muestra `PAN-URL-DB`.

```
admin@M-600> show system info  hostname: M-600 ip-address:
 1.2.3.4 public-ip-address: netmask: 255.255.255.0 default-
gateway: 1.2.3.1 ipv6-address: unknown ipv6-link-local-
address: fe80:00/64 ipv6-default-gateway: mac-address:
 00:56:90:e7:f6:8e time: Mon Apr 27 13:43:59 2015 uptime: 10
 days, 1:51:28 family: m model: M-600 serial: 0073010000xxx
 sw-version: 7.0.0 app-version: 492-2638 app-release-date:
 2015/03/19 20:05:33 av-version: 0 av-release-date: unknown
 wf-private-version: 0 wf-private-release-date: unknown
 wildfire-version: 0 wildfire-release-date: logdb-version:
 7.0.9 platform-family: m pan-url-db: 20150417-220 system-
mode: Pan-URL-DB operational-mode: normal licensed-device-
capacity: 0 device-certificate-status: Ninguno
```

3. Para verificar la versión de la base de datos en la nube en el dispositivo, use el comando **`show pan-url-cloud-status`**.

   El campo `pan-url-db` en la pantalla de información del sistema contiene la misma información.

STEP 5 | Instale las actualizaciones de contenido y base de datos.

El dispositivo solo almacena la versión del contenido que se está ejecutando actualmente y una versión anterior.

Elija uno de los siguientes métodos de instalación:

- Si el servidor PAN-DB tiene acceso directo a Internet, use los siguientes comandos:
  - Para comprobar si se ha publicado una nueva versión: **request pan-url-db upgrade check**
  - Para comprobar la versión que está actualmente instalada en su servidor: **request pan-url-db upgrade info**.
  - Para descargar la última versión: **request pan-url-db upgrade download latest**.

    Para instalar la última versión: **request pan-url-db upgrade install <*version latest | file*>**.
  - Para programar el dispositivo para que busque actualizaciones automáticamente: **set deviceconfig system update-schedule pan-url-db recurring weekly action download-and-install day-of-week <*day of week*> at <*hr:min*>**.
- Si el servidor PAN-DB está fuera de línea, acceda al sitio web de atención al cliente de Palo Alto Networks para descargar y guardar actualizaciones de contenido en un servidor SCP en su red. Entonces podrá importar e instalar las actualizaciones usando los siguientes comandos:
  - **scp import pan-url-db remote-port <*port-number*> from username@host:path**
  - **request pan-url-db upgrade install file <*filename*>**

STEP 6 | Configuración del acceso administrativo a la nube privada de PAN-DB.

El dispositivo tiene una cuenta `admin` predeterminada. Cualquier usuario administrativo adicional que cree puede ser un superusuario (con acceso completo) o superusuario con acceso de solo lectura.

La nube privada de PAN-DB no admite el uso de VSA de RADIUS. Si los VSA empleados en el cortafuegos o Panorama se usan para habilitar el acceso a la nube privada de PAN-DB, se producirá un fallo de autenticación.

- Para configurar un usuario administrativo local en el servidor PAN-DB, utilice los siguientes comandos:
  1. **`configure`**
  2. **`set mgt-config users <username> permissions role-based <superreader | superuser> yes`**
  3. **`set mgt-config users <username> password`**
  4. `Introduzca la contraseña:`**`xxxxx`**
  5. `Confirm password:`**`xxxxx`**
  6. **`commit`**
- Para configurar un usuario administrativo con autenticación RADIUS, utilice los siguientes comandos:
  1. Para crear un perfil de servidor RADIUS: **`set shared server-profile radius <server_profile_name> server <server_name> ip-address <ip_address> port <port_no> secret <shared_password>`**.
  2. Para crear un perfil de autenticación: **`set shared authentication-profile <auth_profile_name> user-domain <domain_name_for_authentication> allow-list <all> method radius server-profile <server_profile_name>`**.
  3. Para adjuntar el perfil de autenticación a un usuario: **`set mgt-config users <username> authentication-profile <auth_profile_name>`**.
  4. Para confirmar sus cambios: **`commit`**.
- Para ver la lista de usuarios, utilice el comando **`show mgt-config users`**.

STEP 7 | Configure los cortafuegos para acceder a la nube privada de PAN-DB.

Configurar cortafuegos para acceder a la nube privada de PAN-DB

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	☐ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada)

¿Dónde puedo usar esto?	¿Qué necesito?
	Nota: *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

Cuando usa la nube pública de PAN-DB, cada cortafuegos accede a los servidores PAN-DB en la nube AWS para descargar la lista de servidores elegibles con los que pueda conectar para las búsquedas de URL. Con la nube privada de PAN-DB, debe configurar los cortafuegos con una lista (estática) de sus servidores de nube privada de PAN-DB que se usarán para las búsquedas de URL. La lista puede contener hasta 20 entradas; se admiten las direcciones IPv4, direcciones IPv6 y FQDN. Cada entrada de la lista (dirección IP o FQDN) debe asignarse al puerto de gestión y/o eth1 del servidor PAN-DB.

STEP 1 | Desde la CLI de PAN-OS, agregue una lista de servidores de nube privada de PAN-DB estáticos que se utilizan para búsquedas de URL.

- Utilice el siguiente comando de la CLI para añadir las direcciones IP de los servidores PAN-DB privados:

```
> configure
```

```
# set deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

Como alternativa, en la interfaz web de cada cortafuegos, seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID (ID de contenido)**, edite la sección Filtrado de URL y, a continuación, introduzca las direcciones IP o los FQDN de los servidores PAN-DB. La lista debe estar separada por comas.

- Para eliminar las entradas de los servidores PAN-DB privados, utilice el siguiente comando:

```
# delete deviceconfig setting pan-url-db cloud-static-list <IP addresses>
```

La eliminación de la lista de servidores PAN-DB privados desencadena un proceso de reelección en el cortafuegos. El cortafuegos comprueba en primer lugar la lista de servidores de nube privada de PAN-DB y, cuando no puede encontrar uno, el cortafuegos accede a los servidores PAN-DB en la nube AWS para descargar la lista de servidores elegibles con los que pueda conectar.

STEP 2 | Escriba **`# commit`** para guardar los cambios.

STEP 3 | Para verificar que el cambio es efectivo, use el siguiente comando de la CLI en el cortafuegos:

```
> show url-cloud status Cloud status: Up URL database version: 20150417-220
```


Configuración de la autenticación con certificados personalizados en la nube privada de PAN-DB.

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by PAN-OS or Panorama)	❑ Licencia de Advanced URL Filtering (o una licencia de filtrado de URL heredada) ***Nota:*** *Las licencias de filtrado de URL heredadas se suspenden, pero las licencias heredadas activas continúan recibiendo soporte.*

De forma predeterminada, un servidor PAN-DB utiliza certificados predefinidos para la autenticación mutua a fin de establecer las conexiones SSL utilizadas para el acceso de gestión y la comunicación entre dispositivos. Sin embargo, puede configurar la autenticación con certificados personalizados en su lugar. Los certificados personalizados le permiten establecer una cadena de confianza única que garantiza la autenticación mutua entre su servidor PAN-DB y sus cortafuegos. En el caso de la nube privada de PAN-DB, el cortafuegos actúa como el cliente y el servidor PAN-DB actúa como el servidor.

STEP 1 | Obtenga pares de claves y certificados de una entidad de certificación (certificate authority, CA) para el servidor PAN-DB y el cortafuegos.

STEP 2 | Importe el certificado de CA para validar el certificado en el cortafuegos.

1. Inicie sesión en la CLI en el servidor PAN-DB e ingrese al modo de configuración.

```
admin@M-600> configure
```

2. Utilice TFTP o SCP para importar el certificado de CA.

```
admin@M-600# {tftp | scp} import certificate from <value>
 file <value> remote-port <1-65535> source-ip <ip/netmask>
 certificate-name <value> passphrase <value> format {pkcs12 |
 pem}
```

STEP 3 | Utilice TFTP o SCP para importar el par de claves que contiene el certificado del servidor y la clave privada para el dispositivo de nube privada.

```
admin@M-600# {tftp | scp} import keypair from <value> file <value>
 remote-port <1-65535> source-ip <ip/netmask> certificate-
name <value> passphrase <value> format {pkcs12 | pem}
```


STEP 4 | Configure un perfil de certificados que incluya la CA de raíz y la CA intermedia. Este perfil de certificado define la autenticación del dispositivo entre el servidor PAN-DB y el cortafuegos.

1. En la CLI del servidor PAN-DB, ingrese al modo de configuración.

```
admin@M-600> configure
```

2. Asigne un nombre al perfil de certificado.

```
admin@M-600# set shared certificate-profile <name>
```

3. (Opcional) Configure el dominio del usuario.

```
admin@M-600# set shared certificate-profile <name>
 domain <value>
```

4. Configure la CA.

   Default-ocsp-url *y* ***ocsp-verify-cert*** *son parámetros opcionales.*

   admin@M-600# **set shared certificate-profile <*name*> CA <*name*>**

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [default-ocsp-url <value>]
```

```
admin@M-600# set shared certificate-profile <name> CA <name>
 [ocsp-verify-cert <value>]
```


STEP 5 | Configure un perfil de servicio SSL/TLS para el dispositivo. Este perfil define el certificado y el alcance del protocolo que utilizan PAN-DB y los dispositivos cliente para los servicios SSL/TLS.

1. Identifique el perfil de servicio SSL/TLS.

```
admin@M-600# set shared ssl-tls-service-profile <name>
```

2. Seleccione el certificado.

```
admin@M-600# set shared ssl-tls-service-profile <name>
 certificate <value>
```

3. Defina el alcance de SSL/TLS.

*PAN-OS 8.0 y las versiones posteriores admiten únicamente TLS versión 1.2 y versiones posteriores. Debe establecer la versión máxima en **TLS 1.2** o **max (máximo)**.*

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings min-version {tls1-0 | tls1-1 | tls1-2
```

```
admin@M-600# set shared ssl-tls-service-profile <name>
 protocol-settings max-version {tls1-0 | tls1-1 | tls1-2 | max
```

STEP 6 | Configure la comunicación segura del servidor en PAN-DB.

1. Establezca el perfil de servicio SSL/TLS. Este perfil se aplica a todas las conexiones SSL entre PAN-DB y los cortafuegos.

```
admin@M-600# set deviceconfig setting management secure-conn-
server ssl-tls-service-profile <ssltls-profile>
```

2. Establezca el perfil de certificado.

```
admin@M-600# set deviceconfig setting management secure-conn-
server certificate-profile <certificate-profile>
```

3. Establezca el tiempo de espera de desconexión. Este es el número de minutos que PAN-DB espera antes de romper y restablecer la conexión con su cortafuegos (el rango es de 0 a 44.640).

```
admin@M-600# set deviceconfig setting management secure-conn-
server disconnect-wait-time <0-44640
```

STEP 7 | Importe el certificado de CA para validar el certificado para el dispositivo.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Importe el certificado de CA.

STEP 8 | Configure un certificado local o de SCEP para el cortafuegos.

1. Si está configurando un certificado local, importe el par de claves para el cortafuegos.
2. Si está configurando un certificado SCEP, configure un perfil SCEP.

STEP 9 | Configure el perfil de certificado para el cortafuegos. Puede configurar esto en cada cortafuegos individualmente o puede enviar esta configuración desde Panorama a los cortafuegos como parte de una plantilla.

1. Seleccione **Device (Dispositivo)** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil de certificado)** para los cortafuegos o **Panorama** > **Certificate Management (Gestión de certificados)** > **Certificate Profile (Perfil del certificado)** para Panorama.
2. Configuración de un perfil de certificado.

STEP 10 | Implemente certificados personalizados en cada cortafuegos. Puede implementar los certificados centralmente desde Panorama o configurarlos manualmente en cada cortafuegos.

1. Inicie sesión en la interfaz web del cortafuegos.
2. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** para un cortafuegos o **Panorama** > **Setup (Configuración)** > **Management (Gestión)** para Panorama y haga clic en **Edit (Editar)** para modificar los ajustes de Comunicación segura.
3. Seleccione el **Certificate Type (Tipo de certificado)**, el **Certificate (Certificado)** y el **Certificate Profile (Perfil de certificado)** del menú desplegable correspondiente.
4. En los ajustes Customize Communication (Personalizar comunicación), seleccione **PAN-DB Communication (Comunicación con PAN-DB)**.
5. Haga clic en **OK (Aceptar)**.
6. Haga clic en **Commit (Confirmar)** para compilar los cambios.

   Tras confirmar los cambios, el cortafuegos no finaliza las sesiones actuales con el servidor PAN-DB hasta después del **Disconnect Wait Time (Tiempo de espera de desconexión)**. El tiempo de espera de desconexión comienza la cuenta atrás después de que aplique la utilización de certificados personalizados en el próximo paso.

STEP 11 | Haga cumplir la autenticación de certificados personalizada.

1. Inicie sesión en la CLI en el servidor PAN-DB e ingrese al modo de configuración.

   ```
   admin@M-600> configure
   ```

2. Aplique la utilización de certificados personalizados.

   ```
   admin@M-600# set deviceconfig setting management secure-conn-
   server disable-pre-defined-cert yes
   ```

Después de confirmar este cambio, el tiempo de espera de desconexión comienza la cuenta atrás (si configuró este ajuste en PAN-DB). Cuando el tiempo de espera finaliza, PAN-DB y su cortafuegos se conectan utilizando únicamente los certificados configurados.

STEP 12 | Existen dos opciones cuando añade nuevos cortafuegos o Panorama a su implementación de nube privada de PAN-DB.

- Si no habilitó **Custom Certificates Only (Certificados personalizados únicamente)**, puede añadir un nuevo cortafuegos a la nube privada de PAN-DB e implementar el certificado personalizado.
- Si habilitó la opción **Custom Certificates Only (Certificados personalizados únicamente)** en la nube privada de PAN-DB, debe implementar los certificados personalizados en los cortafuegos antes de conectarlos a la nube privada de PAN-DB.

