paloalto TECHDOCS

Administración de Advanced DNS Security

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

November 23, 2022

Table of Contents

Acerca de los servicios de suscripción de DNS Security.....5

Medidas de protección y firmas de DNS ofrecidas en la nube.....8

Recopilación y creación de logs de datos.....15

Dominios de servicios regionales.....17

Dominios de servicio regional de DNS Security.....17

Dominios de servicio regional de Advanced DNS Security.....18

Configurar servicios de suscripción de DNS Security..... 21

Habilitación de DNS Security.....22

Habilitar Advanced DNS Security.....36

Configuración de DNS Security sobre TLS.....48

Configurar DNS Security sobre DoH.....50

Crear excepciones de dominio y listas de permitidos | bloqueados.....53

Dominios de prueba.....57

Prueba de conectividad a los servicios de nube de DNS Security.....61

DNS Security.....61

Advanced DNS Security.....62

Configurar tiempo de espera de búsqueda.....64

DNS Security.....64

Advanced DNS Security.....64

Omitir Servicios de suscripciones de DNS Security.....66

Supervise los servicios de suscripción de DNS Security..... 71

Ver panel de DNS Security.....73

Tarjetas de panel de DNS Security.....73

Ver logs de DNS Security.....81

Acerca de los servicios de suscripción de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Palo Alto Networks® proporciona protección integrada especializada contra amenazas basadas en DNS con dos opciones de suscripción de seguridad: DNS Security y Advanced DNS Security. Estas suscripciones de seguridad en la nube funcionan utilizando bases compartidas con las soluciones de Threat Prevention de Palo Alto Networks para proporcionar una solución de seguridad DNS integral y, como tal, requieren la presencia de una suscripción de Advanced Threat Prevention o Threat Prevention.

El servicio en la nube DNS Security diseñado para proteger a su organización contra multitud de amenazas avanzadas basadas en DNS. Al aplicar el aprendizaje automático avanzado y el análisis predictivo a una amplia gama de fuentes de inteligencia de amenazas, DNS Security genera rápidamente firmas DNS mejoradas para defenderse frente a las categorías DNS maliciosas conocidas, así como un análisis en tiempo real de las solicitudes de DNS para defender su red frente a dominios maliciosos recién generados y desconocidos. DNS Security puede detectar varias amenazas DNS, incluidas la tunelización de DNS, los ataques de reenlace de DNS, los dominios creados mediante generación automática, hosts de malware y mucho más.

Con una solución activa de prevención de amenazas que opera en plataformas de seguridad de red compatibles, los clientes pueden redirigir y controlar las solicitudes de DNS utilizando una lista de dominios generados por Palo Alto Networks. Estas listas de firmas de DNS vienen con los paquetes de actualizaciones del antivirus y de WildFire e incluyen las amenazas más pertinentes en el momento de la publicación para permitir la protección y la correcta aplicación de las políticas. Puede acceder a estas listas de forma local y también puede personalizarlas. Para mejorar la cobertura contra las amenazas que utilizan DNS, la suscripción a DNS Security franquea a los usuarios el acceso en tiempo real a las medidas de protección generadas a partir del análisis predictivo avanzado. Identifique de forma proactiva las amenazas ocultas en el tráfico de DNS y comparta los resultados mediante un servicio en la nube con escalabilidad infinita que aplica técnicas como la detección de algoritmos de generación de dominios (domain generation algorithm, DGA), la detección de tunelización de DNS y el aprendizaje automático. Como las medidas de protección y las firmas de DNS se almacenan en una arquitectura basada en la nube, disfruta de acceso a la base de datos completa (y en continua ampliación) de firmas generadas a partir de numerosos orígenes de datos. Así dispone de una defensa en tiempo real contra las diversas amenazas por DNS que plantean los dominios malintencionados recién generados. Para combatir futuras amenazas, se van publicando versiones de contenido que actualizan las funciones de análisis, detección y prevención del servicio.

Para acceder al servicio básico de DNS Security, debe tener una licencia válida de Advanced Threat Prevention o Threat Prevention y una licencia de Advanced DNS Security o DNS Security, además de las licencias base necesarias para operar su plataforma de seguridad de red.

Las suscripciones a DNS Security están disponibles en las siguientes plataformas de seguridad de red de Palo Alto Networks:

- Cortafuegos de nueva generación, incluidas las series VM-Series y CN-Series
- Prisma Access

El servicio Advanced DNS Security es una suscripción complementaria que funciona junto con DNS Security. Esta suscripción adicional permite acceder a nuevos detectores de dominios en la nube de Advanced DNS Security que analiza, en tiempo real, los cambios en las respuestas DNS para detectar distintos tipos de secuestro de DNS. Con el acceso a Advanced DNS Security, que funciona en PAN-OS 11.2 y versiones posteriores, puede detectar y bloquear las respuestas DNS de dominios secuestrados y dominios mal configurados. Los dominios secuestrados y mal configurados pueden introducirse en su red manipulando directamente las respuestas DNS o explotando los ajustes de configuración de la infraestructura DNS de una organización, para redirigir al usuario a un dominio malicioso desde el que pueden iniciar ataques adicionales. La diferencia principal entre estas dos técnicas es dónde se produce la vulnerabilidad. En el caso del secuestro de DNS, el atacante obtiene la capacidad de resolver consultas DNS a dominios operados por atacantes al vulnerar algún aspecto de la infraestructura DNS de una organización, ya sea el acceso administrativo del proveedor de DNS, un ataque MiTM durante el proceso de resolución DNS o el propio servidor DNS. Los dominios mal configurados presentan un problema similar; el atacante busca incorporar su propio dominio malicioso en el DNS de una organización, aprovechando los problemas de configuración del dominio, registros DNS obsoletos que permiten a los atacantes tomar posesión del subdominio del cliente.

Advanced DNS Security puede detectar y catalogar dominios secuestrados y mal configurados en tiempo real mediante el funcionamiento de motores de detección basados en la nube, que proporcionan soporte de integridad de DNS mediante el análisis de las respuestas DNS utilizando análisis basados en aprendizaje automático para detectar actividad maliciosa. Debido a que estos detectores se encuentran en la nube, es posible acceder a una amplia gama de mecanismos de detección que se actualizan y se implementan automáticamente sin necesidad de que el usuario descargue paquetes de actualización cuando se realizan cambios en los detectores. Tras el lanzamiento inicial, Advanced DNS Security es compatible con dos motores de análisis: Dominios con errores de configuración de DNS y dominios de secuestro. Además, las respuestas DNS para todas las consultas DNS se envían a la nube de Advanced DNS Security para un análisis de respuesta mejorado, para catalogar y devolver un resultado con mayor precisión en un intercambio en tiempo real. Los modelos de análisis se entregan a través de actualizaciones de contenido, sin embargo, las mejoras a los modelos existentes se realizan como una actualización del lado de la nube, que no requiere actualización del cortafuegos. Advanced DNS Security se habilita y configura a través del perfil Anti-Spyware (o DNS Security) y requiere licencias activas de Advanced DNS Security y Advanced Threat Prevention (o Threat Prevention).

Para acceder al servicio de Advanced DNS Security, debe tener una licencia de Advanced Threat Prevention o Threat Prevention, y una licencia de Advanced DNS Security válidas, además de las licencias base necesarias para operar su plataforma de seguridad de red.

Las suscripciones de Advanced DNS Security están disponibles en las siguientes plataformas de seguridad de red de Palo Alto Networks:

- Cortafuegos de nueva generación, incluidas las series VM-Series y CN-Series

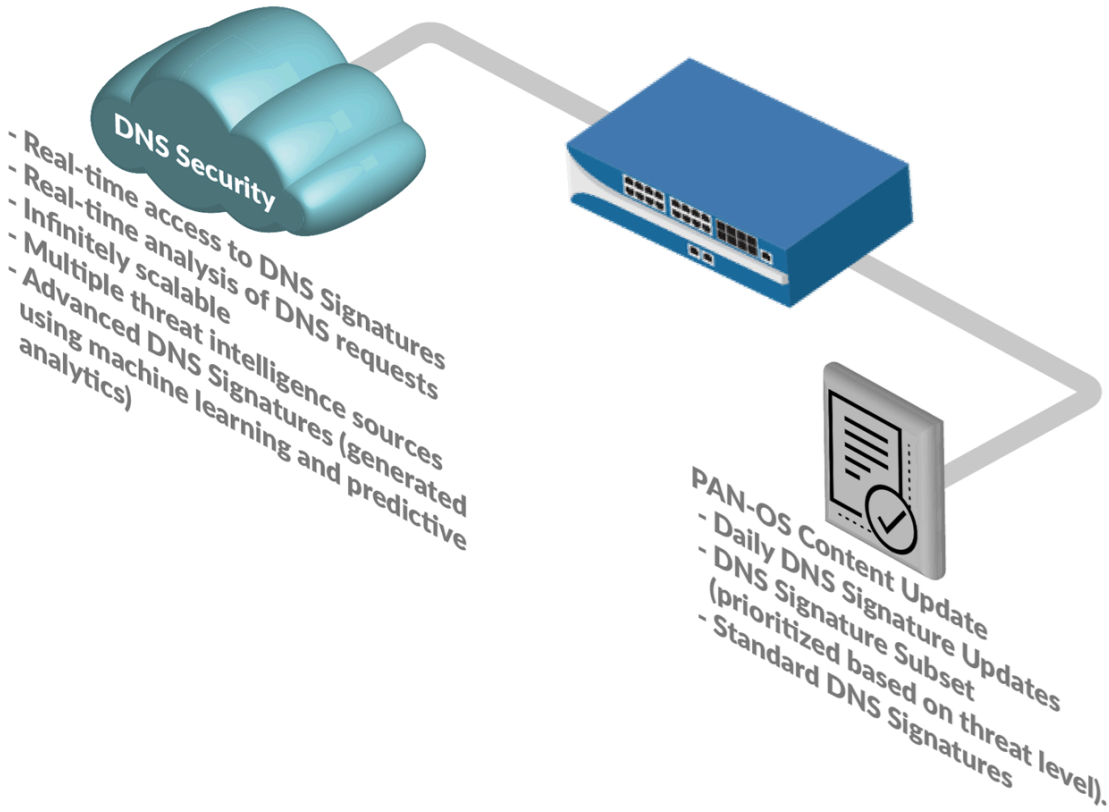
Obtenga más información sobre la implementación y supervisión de DNS Security y Advanced DNS Security en su red:

- Configurar servicios de suscripción de DNS Security
- Supervise los servicios de suscripción de DNS Security

Medidas de protección y firmas de DNS ofrecidas en la nube

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Como servicios basados en la nube, Advanced DNS Security y DNS Security le permiten acceder a una firma DNS infinitamente escalable y a una fuente de protecciones para defender su organización frente a dominios maliciosos. Palo Alto Networks genera las medidas de protección y las firmas de dominios a partir de multitud de orígenes, entre otros, análisis del tráfico con WildFire, DNS pasivo, rastreo activo de internet, análisis de contenido web malintencionado, análisis del entorno de pruebas de URL, redes trampa, inversión del diseño de los algoritmos de generación de dominios (domain generation algorithm, DGA), datos de telemetría, búsquedas con WHOIS, equipo de investigación Unidad 42 y orígenes de datos externos, como Cyber Threat Alliance. Esta base de datos en la nube bajo demanda franquea a los usuarios el acceso a todo el conjunto de firmas de DNS de Palo Alto Network, incluidas las que se generan con técnicas avanzadas de análisis y con análisis en tiempo real de solicitudes de DNS. Los conjuntos de firmas de DNS se pueden descargar para disponer de ellos en una ubicación local. Se incluyen en los paquetes de actualizaciones del antivirus y de WildFire, con un límite fijo de 100 000 firmas. No se incluyen las firmas generadas mediante análisis avanzados. Para facilitar la entrada de las firmas de DNS nuevas que se generan a diario, la base de datos en la nube franquea a los usuarios el acceso instantáneo a las firmas recién añadidas, lo que ahorra descargar las actualizaciones. Si la red se queda sin conexión o deja de estar disponible por cualquier otro motivo, el cortafuegos utiliza el conjunto de firmas de DNS descargado.



El servicio de seguridad de DNS realiza un análisis de solicitudes de DNS en tiempo real mediante análisis predictivos y aprendizaje automático en varias fuentes de datos DNS. Esto se utiliza para generar protecciones para amenazas basadas en DNS a las que se puede acceder en tiempo real mediante la configuración del perfil de seguridad antispyware conectado a una regla de la política de seguridad. Cada categoría de amenaza DNS (el origen de firma DNS) le permite definir acciones de política independientes, así como un nivel de gravedad de log para un tipo de firma específico. Esto le permite crear políticas de seguridad específicas basadas en la naturaleza de la amenaza de acuerdo con los protocolos de seguridad de su red. Palo Alto Networks también genera y mantiene una lista de dominios explícitamente permitidos basada en métricas de PAN-DB y Alexa. Estos dominios de listas permitidas son de acceso frecuente y se sabe que no tienen contenido malicioso. Las categorías de DNS Security y la lista de permitidos se actualizan y se pueden ampliar a través de las publicaciones de contenido de PAN-OS.

PAN-OS 9.1 y versiones anteriores tienen un rango limitado de categorías de fuentes de DNS Security.

DNS Security y Advanced DNS Security actualmente admiten la detección de las siguientes categorías de amenazas de DNS:

El número de ID de amenaza universal (indicado como ID en los logs de amenazas) se asigna a un mecanismo de detección de DNS específico utilizado por DNS Security para clasificar dominios. Esto muestra la categorización precisa del dominio, junto con la categoría de amenaza ampliamente definida, a la que pertenece.

- **Command and Control Domains (Dominios de comando y control)**: C2 incluye URL y dominios utilizados por malware o sistemas comprometidos para comunicarse encubiertamente con el servidor remoto de un atacante y recibir comandos maliciosos o robar datos (esto incluye la detección de túnel DNS y la detección DGA) o agotar recursos en un servidor DNS autorizado de destino (como NXNSattack).
  - **Detección de túnel DNS** (UTID: 109001001/109001002): los atacantes pueden utilizar la tunelización del sistema de nombres de dominio (domain name system, DNS) para codificar dentro de las consultas y las respuestas de DNS los datos de programas y protocolos ajenos a dicho sistema. Así abren un canal trasero con el que pueden transferir archivos o acceder de forma remota al sistema. La detección de túneles de DNS emplea el aprendizaje automático para analizar las cualidades de comportamiento de las consultas de DNS, que incluyen análisis de frecuencia de n-gramas, entropía, frecuencia de consultas y patrones para determinar si las consultas coinciden con ataques basados en la tunelización de DNS. Esto incluye cierto malware de túnel de DNS de próxima generación que roba datos lentamente a través de múltiples dominios para evitar la detección, como TriFive y Snugy. Si se combina con las acciones automatizadas de las políticas del cortafuegos, permite detectar al instante el tráfico de comando y control (command-and-control, C2) o el robo de datos que se ocultan en los túneles de DNS, así como bloquearlos automáticamente en función de las reglas de las políticas definidas.

    Los dominios que se determinan como capaces de realizar una tunelización de DNS son analizados en mayor profundidad para proporcionar detalles sobre las herramientas utilizadas para incrustar datos en las consultas y respuestas DNS, así como el nombre de la campaña de malware asociada, según DNS Security. Los detalles de atribución están disponibles en los logs de amenazas como ID o nombre de amenaza para el cortafuegos y los logs de DNS Security en Prisma Access como Threat Name Firewall (nombre de amenaza escrita por el cortafuegos) utilizando el siguiente formato: Tunelización:<*optional_list_of_tools/campaigns*; cadena separada por puntos)>:<*domain_name*> o Tunneling_infil:*optional_list_of_tools/campaigns*; cadena separada por puntos)>:<*domain_name*> en función del tipo de dominio de túnel DNS específico.
  - **Detección de dominio DGA** (UTID: 109000001): los algoritmos de generación de dominios (domain generation algorithm, DGA) se emplean para generar dominios (por lo general, en grandes cantidades) de forma automática con el fin de establecer un canal malintencionado de comunicaciones de comando y control (command-and-control, C2). El malware basado en DGA (como Pushdo, Bankpatch y CryptoLocker) limita los dominios que se bloquean ocultando la ubicación de sus servidores de C2 activos entre un elevado número de posibles sospechosos. Se puede generar con algoritmos basados en distintos factores, como la hora, las claves criptográficas, los esquemas de nomenclatura derivados del diccionario y otros valores únicos. Aunque la mayoría de los dominios generados con DGA no se resuelve, es preciso identificar todos para ofrecer una defensa integral contra amenazas concretas. El análisis de DGA determina la probabilidad de que el dominio se haya generado de forma automática, no manual. Para ello, se invierte el diseño y se analizan otras técnicas que se suelen emplear en los DGA. Palo Alto Networks se sirve de estas características para identificar y bloquear en tiempo real las amenazas basadas en DGA ya conocidas.
  - **NXNSAttack** (UTID: 109010007): la vulnerabilidad de NXNSAttack presente en el protocolo DNS afecta a todos los solucionadores de DNS recursivos y los actores malintencionados pueden utilizarla para lanzar ataques de amplificación similares a DDOS e interrumpir el funcionamiento normal de los servidores DNS autoritativos vulnerables. NXNSAttack puede introducir picos de tráfico masivos en un servidor DNS autoritativo obligando al solucionador de DNS recursivo a emitir una gran cantidad de solicitudes no válidas para cerrar potencialmente el servidor.

    - **Reenlace de DNS** (UTID: 109010009): los ataques de reenlace DNS atraen a los usuarios a un dominio controlado por el atacante y configurado con un parámetro TTL corto para manipular cómo se resuelven los nombres de dominio a fin de explotar y omitir la política del mismo origen en los navegadores. Esto permite a los actores malintencionados utilizar el equipo cliente como intermediario para atacar o acceder a un recurso contenido en una red privada.
    - **Infiltración de DNS** (UTID: 109001003): la infiltración de DNS incluye consultas DNS que permiten a los actores malintencionados ocultar y resolver cargas útiles diminutas a través de una respuesta a solicitudes de registros A (IPv4) y AAAA (IPv6) fraudulentas. Cuando el cliente resuelve varios subdominios, cada uno de los cuales contiene un registro A/AAAA con un componente codificado, los datos contenidos en ellos se pueden consolidar para formar una carga útil maliciosa, que luego se puede ejecutar en la máquina cliente. Después de ejecutar la carga útil, puede introducir cargas útiles secundarias para establecer un túnel DNS o exploits adicionales.
    - **Generación de perfiles de tráfico DNS** (UTID: 109010010): (Requiere Advanced DNS Security) La generación de perfiles de tráfico DNS es un analizador basado en la nube que detecta malware que intenta establecer una conexión C2, en función de una evaluación de los patrones de tráfico de DNS. A medida que Advanced DNS Security supervisa el tráfico DNS de su organización, las secuencias de solicitud DNS salientes se vectorizan para formar perfiles de tráfico DNS, que luego se analizan mediante técnicas de aprendizaje automático que pueden asociar los patrones de solicitud DNS únicos con perfiles de dominio C2 maliciosos identificables.
- **Dominios alojados en el DNS dinámico** (UTID: 109020002): los servicios DDNS (Dynamic DNS, DNS dinámico) proporcionan una asignación entre los nombres de host y las direcciones IP casi en tiempo real para seguir cambiando las direcciones IP vinculadas a un dominio específico cuando las IP estáticas no estén disponibles. Esto proporciona a los atacantes un método para infiltrarse en las redes mediante el uso de servicios DDNS para cambiar las direcciones IP que albergan los servidores de comando y control. Las campañas de malware y los kits de explotación pueden utilizar los servicios DDNS como parte de su estrategia de distribución de carga útil. Al utilizar dominios DDNS como parte de su infraestructura de nombre de host, los atacantes pueden cambiar la dirección IP asociada con registros DNS determinados y evitar la detección más fácilmente. DNS Security detecta la explotación de los servicios DDNS mediante el filtrado y la referencia cruzada de datos DNS de varios orígenes para generar listas de candidatos que luego se validan para maximizar la precisión.
- **Dominios de malware**: los dominios maliciosos alojan y distribuyen malware, y pueden incluir sitios web que intentan instalar diversas amenazas (como archivos ejecutables, scripts, virus o descargas no autorizadas). Los dominios maliciosos se distinguen de los dominios C2 en que envían cargas útiles maliciosas a su red a través de un origen externo, mientras que con C2, los endpoints infectados normalmente intentan conectarse a un servidor remoto para recuperar instrucciones adicionales u otro contenido malicioso.
    - **DNS comprometido de malware** (UTID: 109003001): el DNS comprometido por malware cubre una variedad de técnicas, algunas legítimas, que provocan la generación de nombres de host y subdominios aparentemente genuinos, que en realidad, son maliciosos. Esto incluye nombres de host recién observados que imitan nombres de host existentes y de buena reputación, en un intento de suplantar o engañar y evadir soluciones de seguridad centradas en la base de datos. Estos se pueden producir rápidamente en masa para evitar su adición a las listas de bases de datos. El enmascaramiento de dominio generalmente sigue después de que un atacante obtiene el control de una cuenta de dominio a través de un ataque más convencional. Esto proporciona el acceso necesario

para crear subdominios ilegítimos utilizados para coordinar ataques, aunque el dominio raíz siga siendo legítimo y válido, lo que aumenta la probabilidad de eludir la seguridad de la red.

  - **Dominios de ransomware** (UTID: 109003002): el ransomware es una subcategoría de malware que bloquea o impide criptográficamente que los usuarios accedan a los datos a cambio del pago de un rescate, después de lo cual el atacante puede devolver el sistema al usuario. El ransomware puede distribuirse a través de dominios de ransomware maliciosos, que alojan los archivos aparentemente legítimos que los usuarios descargan.

- **Dominios recién registrados** (UTID: 109020001): los dominios recién registrados son dominios que han sido agregados recientemente por un operador de TLD o que han cambiado de propiedad en los últimos 32 días. Aunque se pueden crear nuevos dominios con fines legítimos, la gran mayoría se usa a menudo para facilitar actividades maliciosas, como operar como servidores C2 o para usarse para distribuir malware, spam o PUP/adware. Palo Alto Networks detecta los dominios recién registrados mediante la supervisión de feeds específicos (logs de dominio y registradores) y el uso de archivos de zona, DNS pasivo y datos de WHOIS para detectar campañas de registro.
- **Dominios de phishing** (UTID: 109010001): los dominios de phishing intentan atraer a los usuarios para que envíen datos confidenciales, como información personal o credenciales de usuario, haciéndose pasar por sitios web legítimos mediante phishing o pharming. Estas actividades maliciosas se pueden realizar a través de campañas de ingeniería social (mediante las que un origen aparentemente fiable manipula a los usuarios para que envíen información personal por correo electrónico u otras formas de comunicaciones electrónicas) o mediante la redirección del tráfico web, que dirige a los usuarios a sitios fraudulentos que parecen legítimos.
- **Dominios de grayware** (UTID: 109010002): (disponibles con la instalación de la versión de contenido de PAN-OS 8290 y posteriores). los dominios de grayware generalmente no representan una amenaza de seguridad directa. Sin embargo, pueden facilitar vectores de ataque, producir varios comportamientos indeseables o simplemente pueden contener contenido cuestionable/ofensivo.Estos pueden incluir sitios web y dominios que:
  - Intentan engañar a los usuarios para que otorguen acceso remoto.
  - Aprovechan los subdominios de los servicios populares de alojamiento web y sistema dinámico de nombres de dominio (DDNS) para alojar y distribuir contenido malicioso (**Reputación del subdominio** - UTIDL 109002004).
  - Contienen adware y otras aplicaciones no solicitadas (como mineros de criptomonedas, piratas y programas basura [programas potencialmente no deseados]).
  - Implementan acciones de encubrimiento de la identificación del dominio con técnicas de flujo rápido (**fastflux detection** - UTID: 109010005).
  - Demuestran comportamiento y uso maliciosos como se evidencia a través del análisis predicativo de seguridad de DNS (**NRD malicioso** - UTID: 109010006).
  - Redirigen el tráfico de una fuente legítima a un sitio web malicioso debido a un registro DNS configurado incorrectamente u obsoleto en un servidor DNS autorizado que no se ha eliminado o corregido de otra manera (**DNS pendiente** - UTID: 109010008).
  - Promueven actividades ilegales o estafas.
  - Incluyen entradas DNS comodín, que se pueden usar para evadir listas de bloqueo o habilitar ataques DNS comodín enrutando el tráfico a sitios web maliciosos (**abuso de comodines** - UTID: 109002001).
  - Indican la presencia de tráfico DNS con características anómalas en comparación con los perfiles de línea base establecidos creados a partir de los datos DNS recopilados (**detección de anomalías**).

    - Han sido registrados con meses o años de anticipación y dejados en un estado de latencia para eludir los controles de reputación cuando se activan. Esto también incluye dominios recién observados que nunca han sido vistos o evaluados de otra manera (**dominios estratégicamente envejecidos** - UTID: 109002002).
    - Son dominios no utilizados que un atacante ha registrado con probablemente intenciones maliciosas en base a logs de transparencia de certificados (**Detección de dominios almacenados** - UTID: 109002005).
    - Engañan a los usuarios asemejándose a dominios de marcas populares, así como a direcciones de páginas web introducidas incorrectamente, con el objetivo de dirigir a los usuarios a sitios web falsificados y fraudulentos. (**Dominios de ciberocupación / Allanamiento de error tipográfico** - UTID: 109002003).
- **Dominios estacionados** (UTID: 109010003: (disponible con la instalación de la versión de contenido de PAN-OS 8318 y versiones posteriores): los dominios estacionados suelen ser sitios web inactivos que alojan contenido limitado, a menudo en forma de anuncios de clic que pueden generar ingresos para la entidad anfitriona, pero que generalmente no contienen contenido que sea útil para el usuario final. Aunque a menudo funcionan como un marcador de posición legítimo o una simple molestia benigna, también podrían usarse como un posible vector para la distribución de malware.
- **Evasión de proxy y anonimizadores** (UTID: 109010004: (disponible con la instalación de la versión de contenido de PAN-OS 8340 y posterior): la evasión de proxy y anonimizadores hace referencia al tráfico de los servicios que se utilizan para eludir las políticas de filtrado de contenido. Los usuarios que intentan eludir las políticas de filtrado de contenido de una organización a través de los servicios de proxy anonimizador están bloqueados en el nivel de DNS.
- **Dominios de seguimiento de anuncios** (UTID: 109004000): (disponible con la instalación de la versión de contenido 8586 y posteriores de PAN-OS) Los dominios de seguimiento de anuncios ofrecen ciertos tipos de contenido de automatización de marketing para páginas web con el fin de realizar un seguimiento de la participación de los usuarios (como clics en enlaces, navegación por páginas web, etc.). Por lo general, estos dominios de terceros se ocultan mediante el uso de una URL personalizada para que parezca parte del dominio de origen.
    - **Encubrimiento de CNAME** (UTID: 109004001): el encubrimiento de CNAME proporciona un medio alternativo para ocultar una URL modificando una solicitud web para que un subdominio aparezca como si se originara en el mismo sitio web, aunque en realidad, el subdominio utiliza un CNAME para resolverse en un dominio de terceros. Esta técnica elude algunas protecciones de privacidad basadas en el navegador que podrían conectarse a un destino CNAME sospechoso.
- **Dominios secuestrados** (UTID: 109004000): (Requiere Advanced DNS Security) Los dominios secuestrados incluyen dominios en los que los atacantes obtienen la capacidad de hacer que dominios legítimos se dirijan hacia direcciones IP controladas por ellos, generalmente comprometiendo algún aspecto de la infraestructura DNS de una organización. Esto puede incluir el acceso administrativo no autorizado al proveedor de DNS, un ataque MiTM durante el proceso de resolución de DNS o el acceso al propio servidor DNS.
- **Dominios con errores de configuración** (UTID: 109004000): (Requiere Advanced DNS Security) Los dominios con errores de configuración permiten a los atacantes incorporar sus propios dominios malintencionados en el DNS de una organización, aprovechando los problemas de configuración del dominio. Estos registros DNS obsoletos permiten a los atacantes tomar posesión del subdominio del cliente y redirigir a los usuarios a direcciones IP o sitios web controlados por los atacantes con fines malintencionados. Estos dominios con errores de configuración que no se pueden resolver se basan en

los dominios principales orientados al público que se especifican durante la configuración de Advanced DNS Security.

- **Zona de configuración errónea**: (UTID: 109004200): una categoría genérica para dominios con errores de configuración que no corresponden a ninguna otra categoría de configuración incorrecta.
- **Zona de configuración errónea ambigua** (UTID: 109004201): dominios mal configurados que redirigen el tráfico de una fuente legítima a un sitio web malintencionado debido a un registro DNS mal configurado u obsoleto en un servidor DNS autoritativo presente en el dominio público de una organización.
- **NX reclamable de error de configuración** (UTID: 109004202): dominios mal configurados que se definen como parte de la configuración de DNS de una organización, pero que ya no existen (NXDOMAINS), pueden ser registrados a escondidas por los atacantes y usarse para redirigir a los usuarios a sitios web maliciosos y, potencialmente, permiten al atacante obtener acceso a la red de un cliente.

Recopilación y creación de logs de datos

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

El servicio DNS Security recopila información de respuesta y solicitud del servidor en función de las reglas de la política de seguridad, la acción asociada y los detalles de la consulta DNS al realizar búsquedas de dominio para generar logs de DNS Security para aplicaciones de actividad basadas en Strata Logging Service(AIOps for NGFW Free, Prisma Access, Strata Logging Service, etc.). Además, la plataforma de seguridad de red reenvía datos de DNS complementarios a los servidores en la nube de DNS Security y los servicios de Palo Alto Networks los utilizan para proporcionar información de dominio más precisa (como el ASN del proveedor, la información de alojamiento y la identificación de geolocalización). Si bien estos datos complementarios no son necesarios para operar el servicio de seguridad de DNS, proporcionan los recursos para generar mejores capacidades de análisis, detección de DNS y prevención. Esta acción se produce en menos de 30 segundos después de que se produzca la recopilación de datos. Para minimizar el impacto en el rendimiento del cortafuegos, la telemetría de DNS Security funciona con una sobrecarga mínima, lo que puede limitar el volumen total de datos de telemetría DNS enviados a Strata Logging Service; por lo tanto, solo se reenvía un subconjunto de consultas DNS a Strata Logging Service como entradas de registro de DNS Security. Como resultado, Palo Alto Networks recomienda ver los logs de solicitudes de DNS maliciosas como logs de amenazas en lugar de logs de DNS Security.

Las consultas DNS maliciosas también se registran como logs de amenazas y se envían a la carpeta Strata Logging Service mediante el reenvío de logs PAN-OS (cuando se configura correctamente).

DNS Security puede enviar los siguientes campos de datos:

Campo	Description (Descripción)
Acción	Muestra la acción de política tomada en la consulta de DNS.
Tipo	Muestra el tipo de registro DNS.
Respuesta	La dirección IP a la que se resolvió el dominio en la consulta de DNS.
Código de respuesta	El código de respuesta de DNS que se recibió como respuesta a su consulta de DNS.

Campo	Description (Descripción)
IP de origen	La dirección IP del sistema que realizó la solicitud de DNS.
Source User (Usuario de origen)	Cuando la función User-ID del cortafuegos está habilitada, se muestra la identidad del solicitante de DNS.
Zona de origen	La zona de origen configurada a la que se hace referencia en su regla de la política de seguridad.

La recopilación de datos expandida de DNS se omite para los dominios agregados a la lista de permitidos en las excepciones de DNS.

Los campos de datos que se pueden usar para identificar potencialmente a los usuarios (IP de origen, Usuario de origen y Zona de origen) se pueden omitir en el envío automático mediante el siguiente comando de la CLI: **`set deviceconfig setting ctd cloud-dns-privacy-mask yes`**. Debe **`confirmar`** los cambios para que la actualización surta efecto.

Dominios de servicios regionales

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Palo Alto Networks mantiene una red de dominios globales y regionales que proporcionan servicio para operaciones de DNS Security y Advanced DNS Security. Estos dominios de servicio operan analizadores de solicitudes de DNS en tiempo real, acceso a la base de datos de firmas DNS y proporcionan funcionalidad avanzada dependiente de la nube. De forma predeterminada, DNS Security y Advanced DNS Security se conectan a los dominios de servicio globales (dns.service.paloaltonetworks.com y adv-dns.service.paloaltonetworks.com, respectivamente), que luego redirigen automáticamente al dominio regional que está más cerca de la ubicación de la plataforma de seguridad de red.

Dominios de servicio regional de DNS Security

Palo Alto Networks recomienda utilizar la configuración predeterminada del dominio de servicio global para mejorar la gestión de conmutación por error, sin embargo, si experimenta problemas de latencia debido a la singularidad de su ubicación (por ejemplo, cuando se extiende a través de varios dominios regionales superpuestos), puede especificar manualmente el dominio de servicio. Para especificar el dominio de servicio regional utilizado por DNS Security, debe añadir una entrada DNS para dns.service.paloaltonetworks.com que incluya un registro CNAME que indique un dominio regional válido como parte de la configuración del servidor DNS. Después de conectarse a un dominio regional, puede emitir el comando de la CLI en el cortafuegos:

```
show dns-proxy dns-signature counters
```

para revisar la latencia promedio. La sección correspondiente se encuentra en el encabezado API de consulta de firma.

En la tabla siguiente se enumeran los dominios del servicio DNS Security:

Ubicación	URL
Ciudad del Cabo, Sudáfrica	dns-za.service.paloaltonetworks.com
Hong Kong	dns-hk.service.paloaltonetworks.com
Tokio, Japón	dns-jp.service.paloaltonetworks.com

Ubicación	URL
Singapur	dns-sg.service.paloaltonetworks.com
Mumbai, India	dns-in.service.paloaltonetworks.com
Sydney, Australia	dns-au.service.paloaltonetworks.com
Londres, Inglaterra	dns-uk.service.paloaltonetworks.com
Fráncfort, Alemania	dns-de.service.paloaltonetworks.com
Eemshaven, Países Bajos	dns-nl.service.paloaltonetworks.com
París, Francia	dns-fr.service.paloaltonetworks.com
Baréin	dns-bh.service.paloaltonetworks.com
Montreal, Quebec, Canadá	dns-ca.service.paloaltonetworks.com
Osasco, São Paulo, Brasil	dns-br.service.paloaltonetworks.com
Council Bluffs, Iowa, Estados Unidos	dns-us-ia.service.paloaltonetworks.com
Ashburn, Virginia del Norte, EE.UU.	dns-us-va.service.paloaltonetworks.com
The Dalles, Oregón, Estados Unidos	dns-us-or.service.paloaltonetworks.com
Los Ángeles, California, USA	dns-us-ca.service.paloaltonetworks.com

Dominios de servicio regional de Advanced DNS Security

Puede especificar manualmente el servidor que ha utilizado para facilitar las consultas de Advanced DNS Security. Si bien Palo Alto Networks recomienda utilizar el dominio de servicio global predeterminado, puede anular el servidor seleccionado si encuentra una latencia superior a la esperada u otros problemas relacionados con el servicio.

Puede especificar el dominio del servicio Advanced DNS Security en PAN-OS desde **Device (Dispositivo)** > **Setup (Configuración)** > **Management (Gestión)** > **Advanced DNS Security** > **DNS Security Server (Servidor de seguridad DNS)**.

Esta configuración no afecta a la forma en que se gestionan las consultas estándar de DNS Security.

En la tabla siguiente se enumeran los dominios del servicio de Advanced DNS Security:

Ubicación	URL
Ciudad del Cabo, Sudáfrica	za.adv-dns.service.paloaltonetworks.com
Baréin	bh.adv-dns.service.paloaltonetworks.com
Hong Kong	hk.adv-dns.service.paloaltonetworks.com
Tokio, Japón	jp.adv-dns.service.paloaltonetworks.com
Singapur	sg.adv-dns.service.paloaltonetworks.com
Mumbai, India	in.adv.dns.service.paloaltonetworks.com
Sydney, Australia	au.adv-dns.service.paloaltonetworks.com
Londres, Inglaterra	uk.adv-dns.service.paloaltonetworks.com
Fráncfort, Alemania	de.adv.dns.service.paloaltonetworks.com
Eemshaven, Países Bajos	nl.adv.dns.service.paloaltonetworks.com
París, Francia	fr.adv-dns.service.paloaltonetworks.com
Baréin	bh.adv-dns.service.paloaltonetworks.com
Montreal, Quebec, Canadá	ca.adv.dns.service.paloaltonetworks.com
Osasco, São Paulo, Brasil	br.adv.dns.service.paloaltonetworks.com
Council Bluffs, Iowa, Estados Unidos	us-ia.adv.dns.service.paloaltonetworks.com
Ashburn, Virginia del Norte, EE.UU.	us-va.adv.dns.service.paloaltonetworks.com
The Dalles, Oregón, Estados Unidos	us-or.adv.dns.service.paloaltonetworks.com
Los Ángeles, California, USA	us-ca.adv.dns.service.paloaltonetworks.com

Configurar servicios de suscripción de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Antes de habilitar y configurar Advanced DNS Security o DNS Security, debe obtener e instalar una licencia de Threat Prevention (o Advanced Threat Prevention), así como una licencia de Advanced DNS Security o DNS Security, además de cualquier licencia de plataforma desde donde se opere. Las licencias se activan desde el Portal de atención al cliente de Palo Alto Networks y deben estar activas antes de que pueda realizarse el análisis de DNS. Además, los servicios de suscripción de DNS Security (similares a otros servicios de seguridad de Palo Alto Networks) se administran a través de perfiles de seguridad, lo que a su vez depende de la configuración de las políticas de aplicación de red definidas a través de las reglas de las políticas de seguridad. Antes de habilitar un servicio de suscripción de DNS Security, se recomienda que se familiarice con los componentes principales de la plataforma de seguridad en la que se habilitan las suscripciones de seguridad. Consulte su documentación del producto para obtener más información.

Para habilitar y configurar un servicio de suscripción de DNS Security, para que funcione de manera óptima dentro de la implementación de seguridad de red, consulte las tareas a continuación. Si bien puede no ser necesario implementar todos los procesos que se muestran aquí, Palo Alto Networks recomienda revisar todas las tareas para familiarizarse con las opciones disponibles para una implementación correcta. Además, se recomienda que siga las prácticas recomendadas proporcionadas por Palo Alto Networks para una óptima usabilidad y seguridad.

- Habilitar DNS Security o Advanced DNS Security en mi plataforma de seguridad de red para evitar que las amenazas DNS entren en mi red (requerido)
- Cree excepciones de firma de dominio y listas de permitidos que limiten los falsos positivos y eviten que los servidores DNS internos activen la categorización DNS
- Pruebe las acciones de política configuradas para las categorías de dominio disponibles
- Verifique la conectividad de mi cortafuegos con el servicio DNS Security
- Limite las conexiones caídas debido a mi latencia personalizando mi configuración de tiempo de espera de búsqueda DNS en el cortafuegos

Habilitación de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Para habilitar la DNS Security, debe crear (o modificar) un perfil de seguridad Anti-Spyware para acceder al servicio de DNS Security, configurar la gravedad de logs y las configuraciones de políticas para la categoría (o categorías) de firma DNS y luego adjuntar el perfil a una regla de política de seguridad.

- Strata Cloud Manager
- PAN-OS y Panorama

Habilitación de DNS Security (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

STEP 2 | Verifique que una licencia de DNS Security y Threat Prevention (o Advanced Threat Prevention) esté activa. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Overview (Descripción general)** y haga clic en el vínculo Términos de uso de licencia en el panel **License (Licencia)**. Debería ver marcas de verificación verdes junto a los siguientes servicios de seguridad: Antivirus, Antispyware, Protección de vulnerabilidades y DNS Security.

STEP 3 | Compruebe que el App-ID *paloalto-dns-security* de la política de seguridad esté configurado para habilitar el tráfico desde el servicio de seguridad en la nube DNS.

> *Si la implementación del cortafuegos enruta el tráfico de administración a través de un cortafuegos perimetral orientado a Internet y configurado para aplicar políticas de seguridad de App-ID, debe permitir los App-ID en el cortafuegos perimetral; de lo contrario, se impedirá la conectividad de seguridad DNS.*

STEP 4 | Configure los ajustes de la política de firmas de DNS para enviar las consultas de DNS maliciosas al sumidero (sinkhole) definido.

Si utiliza una lista dinámica externa como lista de dominios permitidos, no tiene prioridad sobre las acciones de la política de dominio de seguridad DNS. Como resultado, cuando hay una coincidencia de dominio con una entrada en la categoría de dominio EDL y DNS Security, la acción especificada en DNS Security se sigue aplicando, incluso cuando la EDL se configura explícitamente con una acción de Permitir. Si desea agregar excepciones de dominio DNS, configure una EDL con una acción de alerta o añádalas a la lista de dominios DNS/FQDN permitidos, ubicada en la pestaña de Excepciones DNS.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access** > **Security Services (Servicios de Seguridad)** > **Security Services**.
2. Cree o modifique un perfil de DNS Security existente.
3. En **Name (Nombre)**, especifique el nombre del perfil y, si lo desea, proporcione una descripción.
4. En la sección **DNS Categories (Categorías de DNS)**, debajo del encabezado DNS Security, hay fuentes de firma de DNS configurables individualmente, que le permiten definir acciones de políticas independientes, así como la configuración de captura de paquetes.

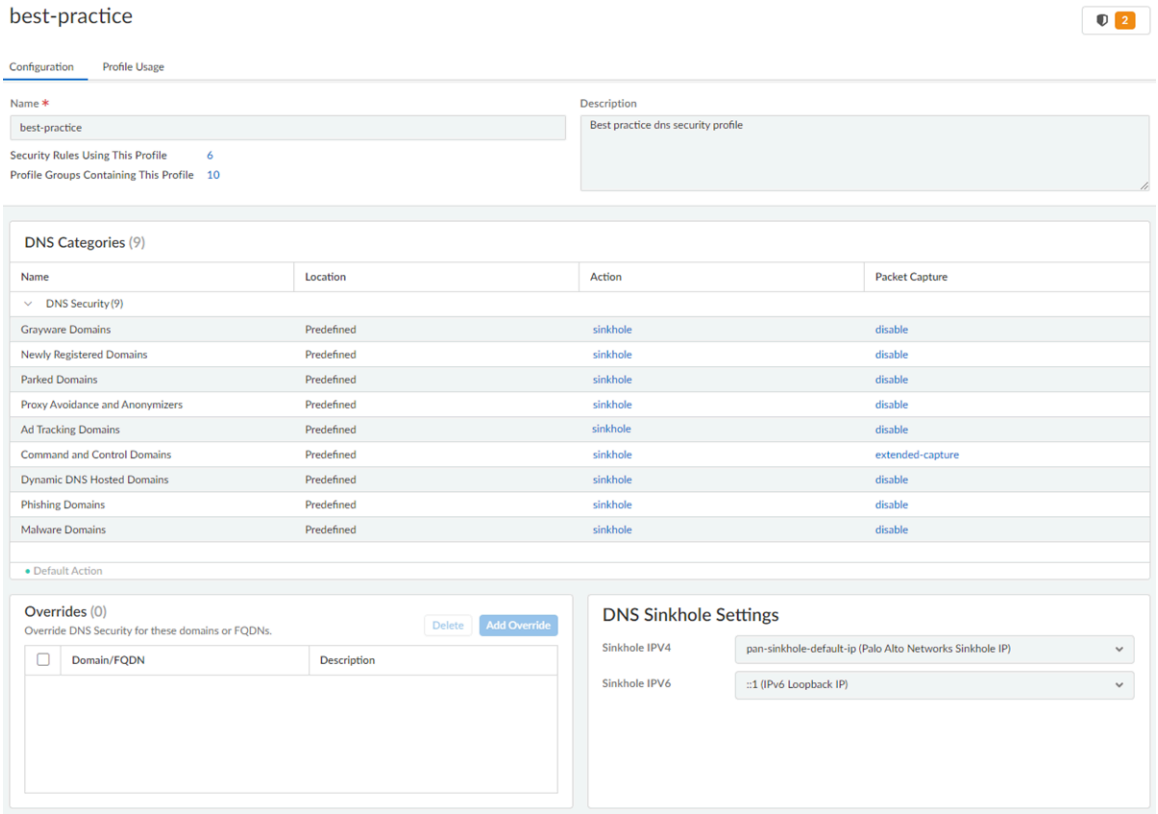
   Palo Alto Networks recomienda utilizar la configuración de acción predeterminada para todas las fuentes de firma, para garantizar una cobertura óptima y ayudar con la respuesta y remediación de incidencias. Para obtener más información sobre las prácticas recomendadas para configurar los ajustes de DNS Security, consulte Prácticas recomendadas para proteger su red de evasiones de Capa 4 y Capa 7.

   - Seleccione la acción que se debe ejecutar cuando se realizan búsquedas de DNS en sitios de malware conocidos con el origen de la firma de DNS Security. Las opciones son alertar, permitir, bloquear o sumidero. Palo Alto Networks recomienda establecer la acción en sinkhole, sumidero.
   - Puede omitir completamente la inspección del tráfico DNS configurando una acción de política de **Permitir** con una gravedad de log correspondiente de **Ninguno** para cada origen de firma DNS.
   - En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.
5. En la sección **DNS Sinkhole Settings (Configuración de sumidero de DNS)**, verifique que exista una dirección de **Sinkhole (Sumidero)** válida. Para su comodidad, la configuración predeterminada (pan-sinkhole-default-ip) está establecida para acceder a un servidor de sumidero

de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección a través de actualizaciones.

Sinkhole (Sumidero) *crea una respuesta a una consulta DNS para dominios que coinciden con la categoría de DNS configurada para una acción de sumidero en el servidor sinkhole especificado, para ayudar a identificar hosts comprometidos. Cuando se utiliza el FQDN de sumidero predeterminado, el cortafuegos envía el registro CNAME como respuesta al cliente, con la expectativa de que un servidor DNS interno resuelva el registro CNAME, lo que permite que las comunicaciones maliciosas del cliente al servidor de sinkhole configurado se registren y sean fácilmente identificables. Sin embargo, si los clientes están en redes sin un servidor DNS interno, o están usando software o herramientas que no pueden resolver adecuadamente un CNAME en una respuesta de registro A, la solicitud de DNS se descarta, lo que genera detalles de log de tráfico incompletos que son cruciales para el análisis de amenazas. En estos casos, deberá utilizar la siguiente dirección IP de sumidero: (72.5.65.111).*

Si desea modificar la dirección de **Sinkhole IPv4** o **Sinkhole IPv6** en un servidor local de su red o en una dirección de bucle invertido, consulte Configuración de la dirección IP de sinkhole en un servidor local o en su red.



6. Haga clic en **OK (Aceptar)** para guardar el perfil de DNS Security.

STEP 5 | Adjunte el perfil de DNS Security a una regla de política de seguridad.

STEP 6 | Compruebe que la acción de política esté forzada.

1. Acceda a los dominios de prueba de DNS Security para verificar que se esté aplicando la acción de política para un tipo de amenaza determinado.
2. Para supervisar la actividad:
    1. Vea los registros de actividad y busque el dominio URL con una acción de sumidero para ver las entradas de log del dominio de prueba al que accedió.

STEP 7 | Opcional: cree una regla de política de descifrado para descifrar el tráfico DNS sobre TLS/puerto 853. Luego, la carga útil del DNS descifrado se puede procesar utilizando la configuración del perfil de DNS Security que contiene la configuración de su política DNS. Cuando se descifra el tráfico DNS sobre TLS, las solicitudes de DNS resultantes en los logs de amenazas aparecerán como una aplicación **dns-base** convencional con un puerto de origen de 853.

STEP 8 | Para otras opciones de supervisión, consulte Supervise los servicios de suscripción de DNS Security

Habilitación de DNS Security (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 y versiones posteriores son compatibles con fuentes de firma DNS configurables individualmente, lo que le permite definir acciones de políticas independientes, así como un nivel de gravedad de logs para un origen de firma determinado. Esto le permite crear acciones de seguridad discretas y precisas basadas en la postura de amenaza de un tipo de dominio según sus protocolos de seguridad de red. Las definiciones de origen de firma DNS son extensibles a través de versiones de contenido de PAN-OS por lo que, cuando se introducen nuevos analizadores de DNS Security, puede crear políticas específicas basadas en la naturaleza de la amenaza. Tras la actualización a PAN-OS 10.0 y posterior, el origen de seguridad DNS se redefine en nuevas categorías para proporcionar controles granulares ampliados; como resultado, las nuevas categorías sobrescribirán la acción definida previamente y adquirirán la configuración predeterminada. Asegúrese de volver a aplicar cualquier configuración de captura de paquetes, gravedad de log y sinkhole adecuados para las categorías de seguridad DNS recién definidas.

- (PAN-OS 11.0 y posterior)
- PAN-OS 10.x
- PAN-OS 9.1

Habilitar DNS Security (PAN-OS 11.0 y posterior)

STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Para aprovechar DNS Security, debe tener una suscripción activa a DNS Security y Threat Prevention (o Advanced Threat Prevention).

Verifique que tenga las suscripciones necesarias. Para verificar las suscripciones para las que tiene licencias actualmente, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas.

STEP 3 | Compruebe que el App-ID *paloalto-dns-security* de la política de seguridad esté configurado para habilitar el tráfico desde el servicio de seguridad en la nube DNS.

Si la implementación del cortafuegos enruta el tráfico de administración a través de un cortafuegos perimetral orientado a Internet y configurado para aplicar políticas de seguridad de App-ID, debe permitir los App-ID en el cortafuegos perimetral; de lo contrario, se impedirá la conectividad de seguridad DNS.

STEP 4 | Configure los ajustes de la política de firmas de DNS para enviar las consultas de DNS maliciosas al sumidero (sinkhole) definido.

Si utiliza una lista dinámica externa como lista de dominios permitidos, no tiene prioridad sobre las acciones de la política de dominio de seguridad DNS. Como resultado, cuando hay una coincidencia de dominio con una entrada en la categoría de dominio EDL y DNS Security, la acción especificada en DNS Security se sigue aplicando, incluso cuando la EDL se configura explícitamente con una acción de Permitir. Si desea agregar excepciones de dominio DNS, configure una EDL con una acción de alerta o añádalas a la lista de dominios DNS/FQDN permitidos, ubicada en la pestaña de Excepciones DNS.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Cree un perfil, modifique uno existente o seleccione uno de los perfiles predeterminados y clónelo.
3. En **Name (Nombre)**, especifique el nombre del perfil y, si lo desea, proporcione una descripción.
4. Seleccione la pestaña **DNS Policies (Políticas DNS)**.
5. En la columna **Signature Source (Origen de firma)**, debajo del encabezado DNS Security (Seguridad DNS), hay orígenes de firma DNS configurables individualmente, que le permiten definir acciones de política independientes, así como un nivel de gravedad de logs.

   Palo Alto Networks recomienda cambiar la configuración predeterminada de las políticas DNS para los orígenes de firmas para garantizar una cobertura óptima, así como para ayudar con la respuesta y corrección de incidencias. Siga las prácticas recomendadas para configurar su configuración de seguridad DNS como se describe en las Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7.

   - Especifique el nivel de gravedad del log que se registra cuando el cortafuegos detecta un dominio que coincide con una firma DNS. Para obtener más información sobre los distintos niveles de gravedad de los logs, consulte Niveles de gravedad de amenazas.
   - Seleccione la acción que se debe ejecutar cuando se realizan búsquedas de DNS en sitios de malware conocidos con el origen de la firma de DNS Security. Las opciones son

predeterminado, permitir, bloquear o sumidero. Verifique que la acción configurada es sinkhole.

- Puede omitir completamente la inspección del tráfico DNS configurando una acción de política de **Permitir** con una gravedad de log correspondiente de **Ninguno** para cada origen de firma DNS.
- En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.

6. En la sección **DNS Sinkhole Settings (Configuración de sumidero de DNS)**, verifique que está habilitada la opción **Sinkhole**. Para su comodidad, la dirección del sinkhole predeterminado (sinkhole.paloaltonetworks.com) está configurada para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección por medio de actualizaciones de contenido.

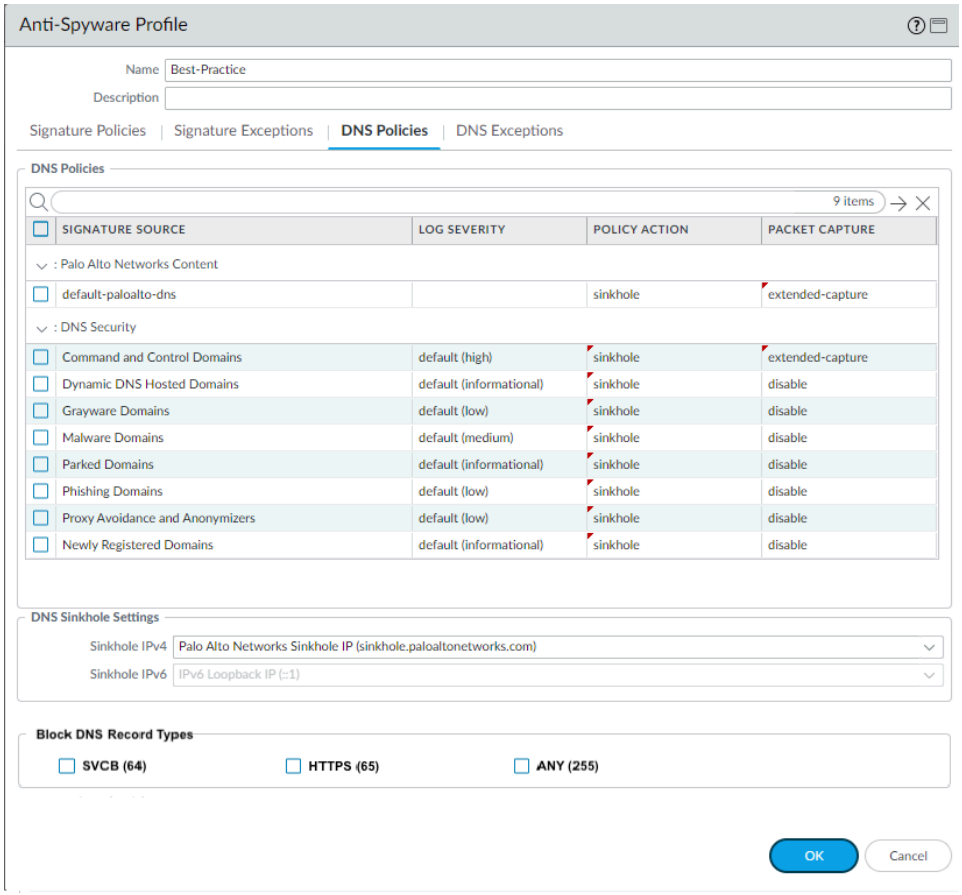
   Sinkhole (Sumidero) *crea una respuesta a una consulta DNS para dominios que coinciden con la categoría de DNS configurada para una acción de sumidero en el servidor sinkhole especificado, para ayudar a identificar hosts comprometidos. Cuando se utiliza el FQDN de sumidero predeterminado (sinkhole.paloaltonetworks.com), el cortafuegos envía el registro CNAME como respuesta al cliente, con la expectativa de que un servidor DNS interno resuelva el registro CNAME, lo que permite que las comunicaciones maliciosas del cliente al servidor de sinkhole de sumidero configurado se registren y sean fácilmente identificables. Sin embargo, si los clientes están en redes sin un servidor DNS interno, o están usando software o herramientas que no pueden resolver adecuadamente un CNAME en una respuesta de registro A, la solicitud de DNS se descarta, lo que genera detalles de log de tráfico incompletos que son cruciales para el análisis de amenazas. En estos casos, deberá utilizar la siguiente dirección IP de sumidero: (72.5.65.111).*

   Si desea modificar la dirección de **Sinkhole IPv4** o **Sinkhole IPv6** en un servidor local de su red o en una dirección de bucle invertido, consulte Configuración de la dirección IP de sinkhole en un servidor local o en su red.

7. (Opcional) Bloquee los tipos de registro de recursos DNS especificados que se utilizan para intercambiar información de claves durante el cifrado del saludo del cliente en la conexión TLS

posterior. Los siguientes tipos de registros de recursos DNS están disponibles: SVCB (64), HTTPS (65) y ANY (255).

- *Si bien no es necesario bloquear ECH para habilitar DNS Security sobre DoH, Palo Alto Networks recomienda actualmente bloquear todos los tipos de registros DNS utilizados por ECH para una seguridad óptima.*
- *Las normas de registro de recursos de los tipos 64 y 65 siguen en evolución (en estado de borrador) y están sujetas a cambios. Para obtener más información sobre DNS SVCB y HTTPS RR, consulte:* Enlace de servicios y especificación de parámetros a través de DNS (SVCB DNS y HTTPS RR) *según lo definido por el* IETF.



8. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

STEP 5 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. En **Security Policy Rule (Regla de política de seguridad)**, seleccione o cree la regla.
3. En la pestaña **Actions (Acciones)**, marque la casilla de verificación **Log at Session End (Crear log al cerrar sesión)** para habilitar la creación de logs.
4. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. En el menú desplegable **Anti-Spyware (Antispyware)**, seleccione el perfil nuevo o modificado.
5. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 6 | Compruebe que la acción de política esté forzada.

1. Acceda a los dominios de prueba de DNS Security para verificar que se esté aplicando la acción de política para un tipo de amenaza determinado.
2. Para supervisar la actividad del cortafuegos:
   1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.
   3. Para más opciones de supervisión, consulte Supervise los servicios de suscripción de DNS Security

STEP 7 | Opcional: cree una regla de política de descifrado para descifrar el tráfico DNS sobre TLS/puerto 853. La carga útil del DNS descifrado se puede procesar utilizando la configuración de perfil antispyware que contiene la configuración de su política DNS. Cuando se descifra el tráfico DNS sobre TLS, las solicitudes de DNS resultantes en los logs de amenazas aparecerán como una aplicación **dns-base** convencional con un puerto de origen de 853.

STEP 8 | Opcional: Ver hosts infectados que intentaron conectar a un dominio malicioso

Habilitar DNS Security (PAN-OS 10.x)

STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Para aprovechar DNS Security, debe tener una suscripción activa a DNS Security y Threat Prevention (o Advanced Threat Prevention).

Verifique que tenga las suscripciones necesarias. Para verificar las suscripciones para las que tiene licencias actualmente, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas.

STEP 3 | Compruebe que el App-ID *paloalto-dns-security* de la política de seguridad esté configurado para habilitar el tráfico desde el servicio de seguridad en la nube DNS.

Si la implementación del cortafuegos enruta el tráfico de administración a través de un cortafuegos perimetral orientado a Internet y configurado para aplicar políticas de seguridad de App-ID, debe permitir los App-ID en el cortafuegos perimetral; de lo contrario, se impedirá la conectividad de seguridad DNS.

STEP 4 | Configure los ajustes de la política de firmas de DNS para enviar las consultas de DNS maliciosas al sumidero (sinkhole) definido.

Si utiliza una lista dinámica externa como lista de dominios permitidos, no tiene prioridad sobre las acciones de la política de dominio de seguridad DNS. Como resultado, cuando hay una coincidencia de dominio con una entrada en la categoría de dominio EDL y DNS Security, la acción especificada en DNS Security se sigue aplicando, incluso cuando la EDL se configura explícitamente con una acción de Permitir. Si desea agregar excepciones de dominio DNS, configure una EDL con una acción de alerta o añádalas a la lista de dominios DNS/FQDN permitidos, ubicada en la pestaña de Excepciones DNS.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Cree un perfil, modifique uno existente o seleccione uno de los perfiles predeterminados y clónelo.
3. En **Name (Nombre)**, especifique el nombre del perfil y, si lo desea, proporcione una descripción.
4. Seleccione la pestaña **DNS Policies (Políticas DNS)**.
5. En la columna **Signature Source (Origen de firma)**, debajo del encabezado DNS Security (Seguridad DNS), hay orígenes de firma DNS configurables individualmente, que le permiten definir acciones de política independientes, así como un nivel de gravedad de logs.

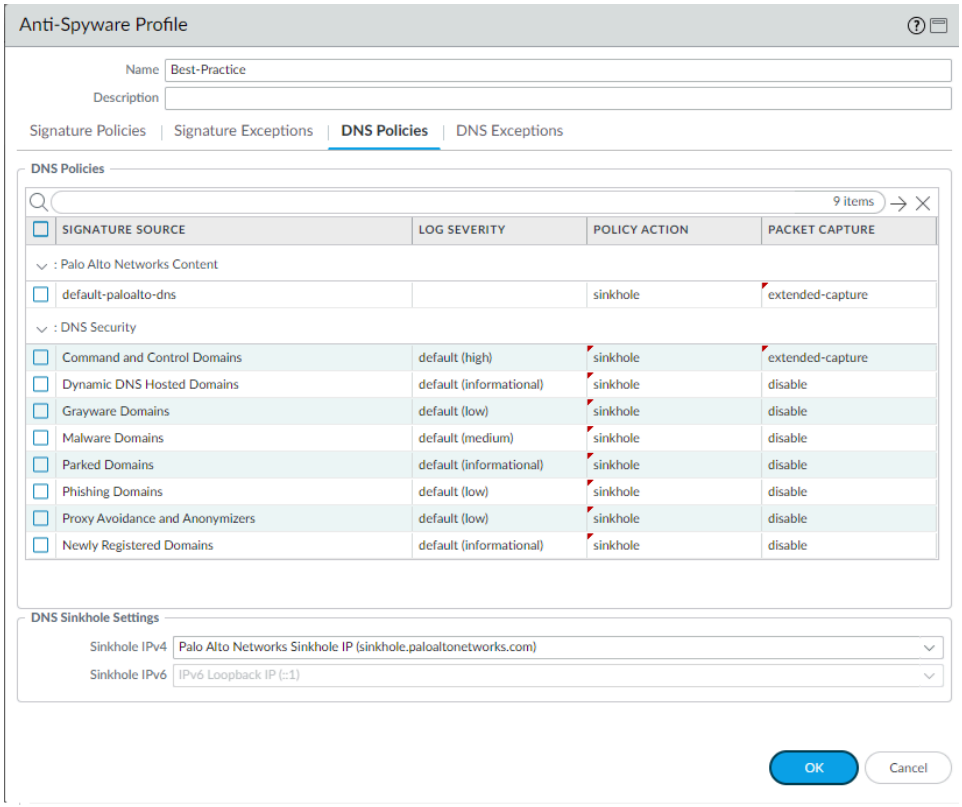
   Palo Alto Networks recomienda cambiar la configuración predeterminada de las políticas DNS para los orígenes de firmas para garantizar una cobertura óptima, así como para ayudar con la respuesta y corrección de incidencias. Siga las prácticas recomendadas para configurar su configuración de seguridad DNS como se describe en las Prácticas recomendadas para proteger su red ante evasiones de capa 4 y capa 7.

   - Especifique el nivel de gravedad del log que se registra cuando el cortafuegos detecta un dominio que coincide con una firma DNS. Para obtener más información sobre los distintos niveles de gravedad de los logs, consulte Niveles de gravedad de amenazas.
   - Seleccione la acción que se debe ejecutar cuando se realizan búsquedas de DNS en sitios de malware conocidos con el origen de la firma de DNS Security. Las opciones son predeterminado, permitir, bloquear o sumidero. Verifique que la acción configurada es sinkhole.
   - Puede omitir completamente la inspección del tráfico DNS configurando una acción de política de **Permitir** con una gravedad de log correspondiente de **Ninguno** para cada origen de firma DNS.
   - En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.
6. En la sección **DNS Sinkhole Settings (Configuración de sumidero de DNS)**, verifique que está habilitada la opción **Sinkhole**. Para su comodidad, la dirección del sinkhole predeterminado (sinkhole.paloaltonetworks.com) está configurada para acceder a un servidor de Palo Alto

Networks. Palo Alto Networks puede actualizar automáticamente esta dirección por medio de actualizaciones de contenido.

Sinkhole (Sumidero) *crea una respuesta a una consulta DNS para dominios que coinciden con la categoría de DNS configurada para una acción de sumidero en el servidor sinkhole especificado, para ayudar a identificar hosts comprometidos. Cuando se utiliza el FQDN de sumidero predeterminado (sinkhole.paloaltonetworks.com), el cortafuegos envía el registro CNAME como respuesta al cliente, con la expectativa de que un servidor DNS interno resuelva el registro CNAME, lo que permite que las comunicaciones maliciosas del cliente al servidor de sinkhole de sumidero configurado se registren y sean fácilmente identificables. Sin embargo, si los clientes están en redes sin un servidor DNS interno, o están usando software o herramientas que no pueden resolver adecuadamente un CNAME en una respuesta de registro A, la solicitud de DNS se descarta, lo que genera detalles de log de tráfico incompletos que son cruciales para el análisis de amenazas. En estos casos, deberá utilizar la siguiente dirección IP de sumidero: (72.5.65.111).*

Si desea modificar la dirección de **Sinkhole IPv4** o **Sinkhole IPv6** en un servidor local de su red o en una dirección de bucle invertido, consulte Configuración de la dirección IP de sinkhole en un servidor local o en su red.



7. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

STEP 5 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. En **Security Policy Rule (Regla de política de seguridad)**, seleccione o cree la regla.
3. En la pestaña **Actions (Acciones)**, marque la casilla de verificación **Log at Session End (Crear log al cerrar sesión)** para habilitar la creación de logs.
4. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. En el menú desplegable **Anti-Spyware (Antispyware)**, seleccione el perfil nuevo o modificado.
5. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 6 | Compruebe que la acción de política esté forzada.

1. Acceda a los dominios de prueba de DNS Security para verificar que se esté aplicando la acción de política para un tipo de amenaza determinado.
2. Para supervisar la actividad del cortafuegos:
   1. Seleccione **ACC** y añada un dominio de URL como filtro global para ver la actividad de amenazas y la actividad bloqueada para el dominio al cual accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.
   3. Para más opciones de supervisión, consulte Supervise los servicios de suscripción de DNS Security

STEP 7 | Opcional: cree una regla de política de descifrado para descifrar el tráfico DNS sobre TLS/puerto 853. La carga útil del DNS descifrado se puede procesar utilizando la configuración de perfil antispyware que contiene la configuración de su política DNS. Cuando se descifra el tráfico DNS sobre TLS, las solicitudes de DNS resultantes en los logs de amenazas aparecerán como una aplicación **dns-base** convencional con un puerto de origen de 853.

STEP 8 | Opcional: Ver hosts infectados que intentaron conectar a un dominio malicioso

Habilitar DNS Security (PAN-OS 9.1)

STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Para aprovechar las ventajas de DNS Security, debe tener una suscripción activa a DNS Security y Threat Prevention.

Verifique que tenga las suscripciones necesarias. Para verificar las suscripciones para las que tiene licencias actualmente, seleccione **Device (Dispositivo)** > **Licenses (Licencias)** y verifique que las licencias correspondientes se muestren y no estén vencidas.

STEP 3 | Compruebe que el App-ID *paloalto-dns-security* de la política de seguridad esté configurado para habilitar el tráfico desde el servicio de seguridad en la nube DNS.

Si la implementación del cortafuegos enruta el tráfico de administración a través de un cortafuegos perimetral orientado a Internet y configurado para aplicar políticas de seguridad de App-ID, debe permitir los App-ID en el cortafuegos perimetral; de lo contrario, se impedirá la conectividad de seguridad DNS.

STEP 4 | Configure los ajustes de la política de firmas de DNS para enviar las consultas de DNS de malware al sinkhole definido.

Si utiliza una lista dinámica externa como lista de dominios permitidos, no tiene prioridad sobre las acciones de la política de dominio de seguridad DNS. Como resultado, cuando hay una coincidencia de dominio con una entrada en la categoría de dominio EDL y DNS Security, la acción especificada en DNS Security se sigue aplicando, incluso cuando la EDL se configura explícitamente con una acción de Permitir. Si desea añadir excepciones de dominio DNS, puede configurar una EDL con una acción de alerta.

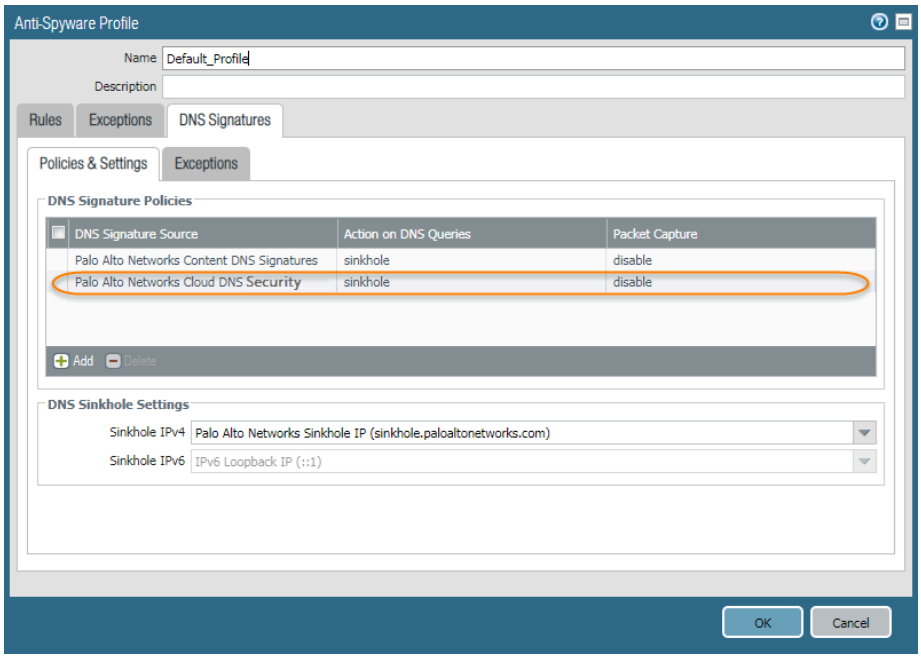
1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Cree un perfil, modifique uno existente o seleccione uno de los perfiles predeterminados y clónelo.
3. En **Name (Nombre)**, especifique el nombre del perfil y, si lo desea, proporcione una descripción.
4. Seleccione la pestaña **DNS Signatures (Firmas de DNS) > Policies & Settings (Políticas y configuración)**.
5. Si no aparece el origen **Palo Alto Networks DNS Security**, haga clic en **Add (Añadir)** y selecciónelo en la lista.
6. Seleccione la acción que se debe ejecutar cuando se realizan búsquedas de DNS en sitios de malware conocidos con el origen de la firma de DNS Security. Las opciones son alertar, permitir, bloquear o sumidero. Verifique que la acción configurada es sinkhole.
7. (Opcional) En la lista desplegable **Packet Capture (Captura de paquetes)**, seleccione **single-packet (un solo paquete)** para capturar el primer paquete de la sesión o **extended-capture (captura extendida)** para configurar entre 1 y 50 paquetes. A continuación, puede usar las capturas de paquete para un análisis más detallado.
8. En la sección **DNS Sinkhole Settings (Configuración de sumidero de DNS)**, verifique que está habilitada la opción **Sinkhole**. Para su comodidad, la dirección del sinkhole predeterminado (sinkhole.paloaltonetworks.com) está configurada para acceder a un servidor de Palo Alto

Networks. Palo Alto Networks puede actualizar automáticamente esta dirección por medio de actualizaciones de contenido.

Sinkhole (Sumidero) *crea una respuesta a una consulta DNS para dominios que coinciden con la categoría de DNS configurada para una acción de sumidero en el servidor sinkhole especificado, para ayudar a identificar hosts comprometidos. Cuando se utiliza el FQDN de sumidero predeterminado (sinkhole.paloaltonetworks.com), el cortafuegos envía el registro CNAME como respuesta al cliente, con la expectativa de que un servidor DNS interno resuelva el registro CNAME, lo que permite que las comunicaciones maliciosas del cliente al servidor de sinkhole de sumidero configurado se registren y sean fácilmente identificables. Sin embargo, si los clientes están en redes sin un servidor DNS interno, o están usando software o herramientas que no pueden resolver adecuadamente un CNAME en una respuesta de registro A, la solicitud de DNS se descarta, lo que genera detalles de log de tráfico incompletos que son cruciales para el análisis de amenazas. En estos casos, deberá utilizar la siguiente dirección IP de sumidero: (72.5.65.111).*

Si desea modificar la dirección de **Sinkhole IPv4** o **Sinkhole IPv6** en un servidor local de su red o en una dirección de bucle invertido, consulte Configuración de la dirección IP de sinkhole en un servidor local o en su red.

9. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.



STEP 5 | Adjunte el perfil de antispyware a una regla de política de seguridad.

1. Seleccione **Policies (Políticas)** > **Security (Seguridad)**.
2. En **Security Policy Rule (Regla de política de seguridad)**, seleccione o cree la regla.
3. En la pestaña **Actions (Acciones)**, marque la casilla de verificación **Log at Session End (Crear log al cerrar sesión)** para habilitar la creación de logs.
4. En la sección Profile Setting, haga clic en el menú desplegable **Profile Type** para ver todos los **Profiles**. En el menú desplegable **Anti-Spyware (Antispyware)**, seleccione el perfil nuevo o modificado.
5. Haga clic en **OK (ACEPTAR)** para guardar la regla de política.

STEP 6 | Compruebe que la acción de política esté forzada.

1. Acceda a los dominios de prueba de DNS Security para verificar que se esté aplicando la acción de política para un tipo de amenaza determinado.
2. Para supervisar la actividad del cortafuegos:
   1. Vea la actividad de amenaza y busque el dominio de prueba de URL y la actividad bloqueada para el dominio al que accedió.
   2. Seleccione **Monitor (Supervisar)** > **Logs** > **Threat (Amenaza)** y filtre por `(action eq sinkhole)` para visualizar los logs en los dominios de sinkhole.
   3. Para más opciones de supervisión, consulte Supervise los servicios de suscripción de DNS Security

STEP 7 | Opcional: cree una regla de política de descifrado para descifrar el tráfico DNS sobre TLS/puerto 853. La carga útil del DNS descifrado se puede procesar utilizando la configuración de perfil antispyware que contiene la configuración de su política DNS. Cuando se descifra el tráfico DNS sobre TLS, las solicitudes de DNS resultantes en los logs de amenazas aparecerán como una aplicación **dns-base** convencional con un puerto de origen de 853.

STEP 8 | Opcional: Ver hosts infectados que intentaron conectar a un dominio malicioso

Habilitar Advanced DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Advanced DNS Security complementa su configuración de seguridad DNS existente para brindar protección adicional frente al secuestro de DNS al inspeccionar los cambios en las respuestas DNS. Debe haber configurado completamente la configuración de DNS Security antes de continuar con este paso.

Para habilitar la Advanced DNS Security, debe crear (o modificar) un perfil de seguridad Anti-Spyware para acceder al servicio de Advanced DNS Security, configurar la gravedad de logs y las configuraciones de políticas para la categoría (o categorías) de firma DNS y luego adjuntar el perfil a una regla de política de seguridad.

- (PAN-OS 11.2 y posterior)
- Gestión de la nube

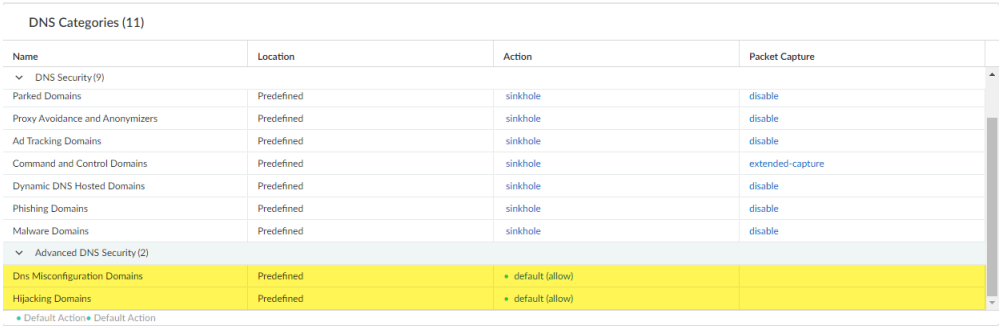
Habilitar Advanced DNS Security (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

STEP 2 | Compruebe que una licencia de DNS Security y Threat Prevention esté activa. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Overview (Descripción general)** y haga clic en el vínculo Términos de uso de licencia en el panel **License (Licencia)**. Debería ver marcas de verificación verdes junto a los siguientes servicios de seguridad: Antivirus, Antispyware, Protección de vulnerabilidades y DNS Security.

STEP 3 | Actualice o cree un nuevo perfil de DNS Security para habilitar las consultas de Advanced DNS Security en tiempo real. Normalmente, este es su perfil de DNS Security existente utilizado para la configuración de DNS Security.

1. Seleccione un perfil de DNS Security existente o seleccione **Add (Añadir)** uno nuevo [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **DNS Security**].
2. Seleccione su perfil de DNS Security y luego vaya a **DNS Categories (Categorías DNS)**.



3. Para cada categoría de dominio de Advanced DNS Security, especifique una **Action (Acción)** de política que debe realizar cuando se detecte un tipo de dominio correspondiente. Actualmente hay dos motores de análisis disponibles: **Dominios con errores de configuración de DNS** y **dominios de secuestro**.

   Opciones de acción de política:

   - **allow (permitir)**: se permite la consulta DNS.

     Puede configurar Strata Cloud Manager para generar una alerta cuando se detecte el tipo de dominio aplicable configurando la acción a permitir y la gravedad de logs en informativo.

   - **block (bloquear)**: la consulta DNS se bloquea.
   - **Sinkhole (Sumidero)**: crea una respuesta DNS para una consulta DNS dirigida a un dominio malicioso detectado. Esto dirige la resolución del nombre de dominio malicioso a una dirección IP específica (denominada IP de sumidero), que se incrusta como la respuesta. La dirección IP de sumidero predeterminada se establece para acceder a un servidor de Palo Alto Networks. Palo Alto Networks puede actualizar automáticamente esta dirección IP a través de actualizaciones de contenido.

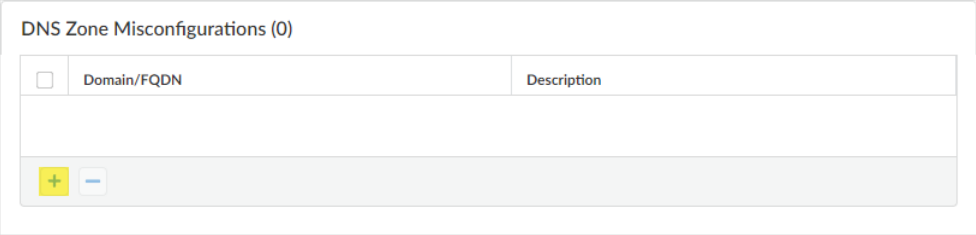
STEP 4 | (Opcional) Especifique cualquier dominio principal orientado al público dentro de su organización que desee que Advanced DNS Security analice y supervise para detectar la presencia de dominios mal configurados. Los dominios mal configurados son creados inadvertidamente por propietarios de dominios que apuntan registros de alias a dominios de terceros usando tipos de registros CNAME,

MX, NS, usando entradas que ya no son válidas, lo que permite a un atacante hacerse con el dominio registrando los dominios caducados o no usados.

Los TLD (dominios de nivel superior) y los dominios de nivel raíz no se pueden añadir a la lista de configuraciones erróneas de la zona DNS.

1. Seleccione un perfil de seguridad DNS [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and Prisma Access (NGFW y Prisma Access)** > **Security Services (Servicios de seguridad)** > **DNS Security**] que contenga una configuración de Advanced DNS Security.
2. En la sección **DNS Zone Misconfigurations (Configuraciones erróneas de la zona DNS)**, agregue dominios principales orientados al público con una descripción opcional para ayudarle a identificar el uso o la propiedad del dominio dentro de su organización.

   Las entradas deben tener un "." incluido en el dominio utilizando el siguiente formato (por ejemplo paloaltonetworks.com), de lo contrario se analiza como un nombre de host, el cual se considera un dominio privado.



3. Haga clic en **OK (Aceptar)** para salir y guardar el perfil de seguridad de DNS Security.

STEP 5 | (Opcional) Supervise la actividad en Strata Cloud Manager para detectar consultas DNS que se hayan detectado mediante Advanced DNS Security. Las categorías de DNS Security analizadas mediante el análisis en tiempo real de Advanced DNS Security del paquete de respuesta DNS tienen el prefijo ‘adns’ seguido de la categoría. Por ejemplo, adns-dnsmisconfig, donde ‘dnsmisconfig’ indica el tipo de categoría de DNS compatible. Si la categoría de dominio DNS se determinó analizando el paquete de solicitud DNS, la categoría especificada se muestra con el prefijo «dns» seguido de la categoría. Por ejemplo, «dns-grayware».

1. Acceda a los dominios de prueba de Advanced DNS Security para comprobar que se está aplicando la acción de política para un tipo de amenaza determinado.
2. Seleccione **Incidents & Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**. Puede filtrar los logs de amenazas en función del tipo específico de categoría de dominio de Advanced DNS Security, por ejemplo `threat_category.value = 'adns-hijacking'`, mediante el cual la variable `adns-hijacking` indica consultas DNS que Advanced DNS Security ha categorizado como un intento de secuestro DNS malicioso. Las siguientes categorías de amenazas de Advanced DNS Security disponibles en los logs:

   Categorías de Advanced DNS Security

   - **Secuestro DNS**: `adns-hijacking`

     Los dominios de secuestro de DNS tienen un ID de amenaza de (UTID: 109.004.100).

- **Configuración errónea de DNS**: `adns-dnsmisconfig`

  los dominios con errores de configuración de DNS tienen tres ID de amenazas, que corresponden a tres variantes de tipos de dominios con errores de configuración de DNS: dnsmisconfig_zone (UTID: 109.004.200), dnsmisconfig_zone_dangling (UTID: 109.004.201), y dnsmisconfig_claimable_nx (UTID: 109,004,202). Puede restringir la búsqueda haciendo referencia cruzada a un valor de ID de amenaza que corresponde a un tipo de dominio de configuración erróea de DNS específico. Por ejemplo, `threat_category.value = 'adns-dnsmisconfig'` y `Threat ID = 109004200`, por lo que 109004200 indica el ID de amenaza de un dominio de configuración incorrecta DNS que no enruta tráfico a un dominio activo debido a un problema de configuración del servidor DNS.

Categorías DNS analizadas mediante el análisis de respuesta mejorado de Advanced DNS Security.

- **DNS** : `adns-benign`
- **Dominios de malware** : `adns-malware`
- **Dominios de comando y control**: `adns-c2`
- **Dominios de phishing**: `adns-phishing`
- **Dominios alojados en el DNS dinámico**: `adns-ddns`
- **Dominios recientemente registrados**: `adns-new-domain`
- **Dominios de Grayware**: `adns-grayware`
- **Dominios estacionados**: `adns-parked`
- **Evasión de proxy y anonimizadores**: `adns-proxy`
- **Dominios de seguimiento de anuncios**: `adns-adtracking`

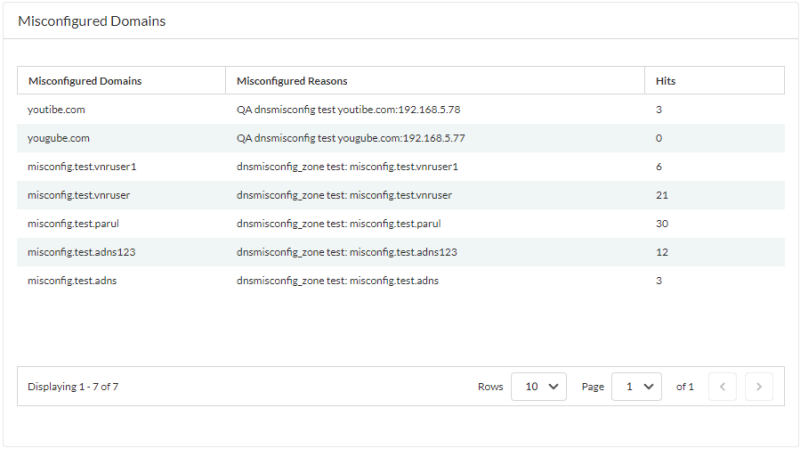
> *Si la consulta DNS no se completa dentro del período de tiempo de espera especificado para Advanced DNS Security, se utilizará la categorización de DNS Security, cuando sea posible. En esos casos, se utiliza la notación heredada para la categoría, por ejemplo, en lugar de `adns-malware`, se clasificará como `dns-malware`, lo que indica que se utilizó el valor de categorización de DNS Security.*

3. Seleccione una entrada de log para ver los detalles de una consulta DNS.
4. La **Category (Categoría)** de DNS se muestra en el panel **General** de la vista de log detallada. Además, puede ver otros aspectos de la amenaza, incluida la URL de origen, el tipo específico de amenaza y las características asociadas.

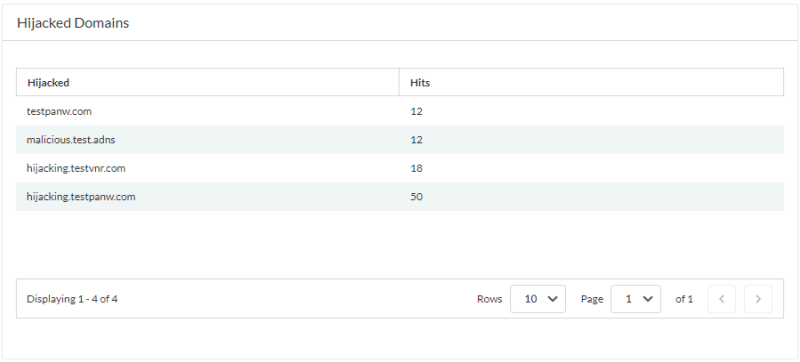
STEP 6 | (Opcional) Recuperar una lista de dominios mal configurados y dominios secuestrados detectados por el servicio de Advanced DNS Security. Los dominios mal configurados se basan en las entradas de dominios principales orientados al público añadidas a **DNS Zone Misconfigurations**.

Las entradas de dominio mal configuradas que se eliminan de la red no se reflejan inmediatamente en las estadísticas del panel de Advanced DNS Security.

1. Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.
2. Seleccione **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **DNS Security** para abrir el panel de DNS Security.
3. Desde el panel de DNS Security, consulte los siguientes widgets:
   - **Misconfigured Domains (Dominios mal configurados)**: vea una lista de dominios que no se pueden resolver asociados con los dominios principales orientados al público especificados por el usuario. Para cada entrada, hay un motivo para la mala configuración y un recuento de resultados de tráfico basado en la IP de origen.



   - **Hijacked Domains (Dominios secuestrados)**: vea una lista de dominios secuestrados determinada por Advanced DNS Security. Para cada entrada, hay un motivo para la clasificación y un recuento de resultados de tráfico basado en la IP de origen.



Habilitar Advanced DNS Security (PAN-OS 11.2 y posterior)

Palo Alto Networks recomienda habilitar la funcionalidad DNS Security antes de configurar Advanced DNS Security.

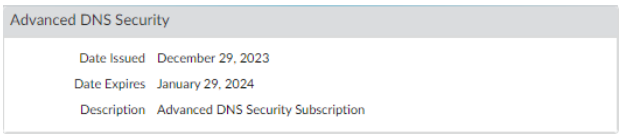
STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Actualice la versión de contenido a 8832 o posterior.

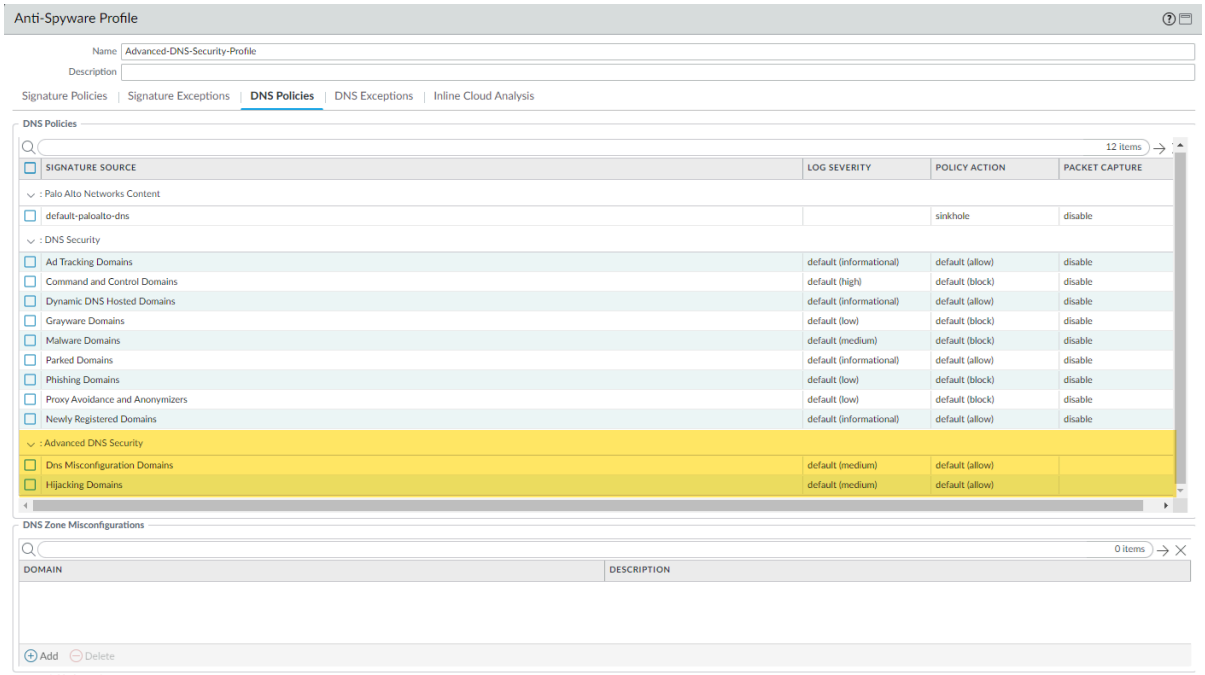
STEP 3 | Para evitar el acceso a dominios maliciosos conocidos y desconocidos mediante Advanced DNS Security, debe tener una licencia de Advanced DNS Security activa. Esto solo debe instalarse después de actualizar a PAN-OS 11.2.

> *Advanced DNS Security admite un modelo de licencia que incorpora la funcionalidad DNS Security en la licencia Advanced DNS Security cuando se instala en un cortafuegos sin licencia anterior. Si actualiza desde un cortafuegos con una licencia DNS Security existente, se mostrarán las entradas que indiquen la presencia de licencias DNS Security y Advanced DNS Security independientes. En esta instancia, la licencia de DNS Security es una entrada pasiva y todas las funcionalidades de DNS Security y Advanced DNS Security se otorgan a través de la licencia Advanced DNS, incluida la fecha de vencimiento pertinente. Los cortafuegos sin una licencia DNS Security instalada previamente muestran una licencia Advanced DNS Security, sin embargo, proporciona funcionalidad DNS Security y Advanced DNS Security.*
>
> *En consecuencia, si cambia a una versión inferior de PAN-OS que opera con una licencia de Advanced DNS Security a una versión que no admite Advanced DNS Security, el cortafuegos continúa mostrando y otorgando funcionalidad de DNS Security a través de la licencia de Advanced DNS Security. Sin embargo, se limita a las características de seguridad DNS básicas.*

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 4 | Actualice o cree un nuevo perfil de Seguridad antispyware para habilitar las consultas de Advanced DNS Security en tiempo real. Normalmente, este es su perfil de seguridad Antispyware existente utilizado para la configuración de DNS Security.



1. Seleccione un perfil de seguridad antispyware existente o seleccione **Add (Añadir)** uno nuevo [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)**].
2. Seleccione su perfil de seguridad antispyware y luego vaya a **DNS Policies (Políticas DNS)**.
3. Para cada categoría de dominio de Advanced DNS Security, especifique la **Log Severity (Gravedad de logs)** y la **Policy Action (Acción de política)** que debe realizar cuando se detecte un tipo de dominio mediante un motor de análisis correspondiente. Actualmente hay dos motores de análisis disponibles: **Dominios con errores de configuración de DNS** y **dominios de secuestro**.

   Opciones de acción de política:

   - **allow (permitir)**: se permite la consulta DNS.

     Puede configurar el cortafuegos para generar una alerta cuando se detecte el tipo de dominio aplicable estableciendo la acción para permitir y la gravedad del log en informativo.

   - **block (bloquear)**: la consulta DNS se bloquea.
   - **Sinkhole (Sumidero)**: crea una respuesta DNS para una consulta DNS dirigida a un dominio malicioso detectado. Esto dirige la resolución del nombre de dominio malicioso a una dirección IP específica (denominada IP de sumidero), que se incrusta como la respuesta. La dirección IP de sumidero predeterminada se establece para acceder a un servidor de Palo Alto Networks. Palo

Alto Networks puede actualizar automáticamente esta dirección IP a través de actualizaciones de contenido.

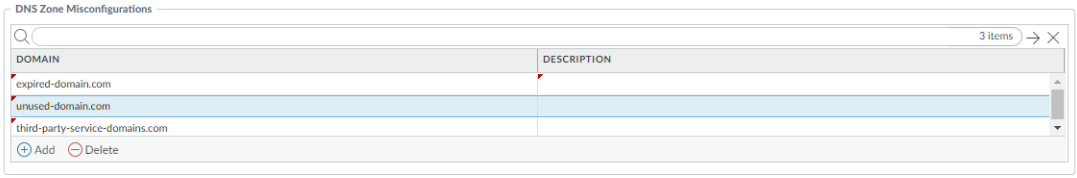
Opciones de Gravedad de logs:

- **none (ninguna)**: el evento no tiene un nivel de gravedad de log asociado.
- **low (baja)**: amenazas con nivel de advertencia que tienen muy poco impacto en la infraestructura de la organización. Suelen requerir acceso local o físico al sistema y con frecuencia suelen ocasionar problemas en la privacidad de las víctimas, problemas de DoS y fugas de información.
- **informational (informativa)**: eventos sospechosos que no suponen una amenaza inmediata, pero que se registran para indicar que podría haber problemas más serios.
- **medium (mediana)**: amenazas menores en las que se minimiza el impacto, como ataques DoS que no comprometen al objetivo o vulnerabilidades que requieren que el atacante esté en la misma LAN que la víctima, afectan solo a configuraciones no estándar o aplicaciones oscuras u ofrecen acceso muy limitado.
- **high (alta)**: amenazas que tienen la habilidad de convertirse en críticas pero que tienen factores atenuantes; por ejemplo, pueden ser difíciles de explotar, no conceder privilegios elevados o no tener un gran grupo de víctimas.
- **critical (crítica)**: amenazas graves, como aquellas que afectan a las instalaciones predeterminadas de software ampliamente implementado, que comprometen profundamente los servidores y dejan el código de explotación al alcance de los atacantes. El atacante no suele necesitar ningún tipo de credenciales de autenticación o conocimientos acerca de las víctimas y el objetivo no necesita ser manipulado para que realice ninguna función especial.

4. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil de seguridad antispyware y en **Commit (Confirmar)** para confirmar sus cambios.

STEP 5 | (Opcional) Especifique cualquier dominio principal orientado al público dentro de su organización que desee que Advanced DNS Security analice y supervise para detectar la presencia de dominios mal configurados. Los dominios mal configurados son creados inadvertidamente por propietarios de dominios que apuntan registros de alias a dominios de terceros usando tipos de registros CNAME, MX, NS, usando entradas que ya no son válidas, lo que permite a un atacante hacerse con el dominio registrando los dominios caducados o no usados.

Los TLD (dominios de nivel superior) y los dominios de nivel raíz no se pueden añadir a la lista de configuraciones erróneas de la zona DNS.



1. Seleccione un perfil de seguridad antispyware [**Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware (Antispyware)**] y vaya a **DNS Policies (Políticas DNS)**.

2. En la sección **DNS Zone Misconfigurations (Configuraciones erróneas de la zona DNS)**, agregue dominios principales orientados al público con una descripción opcional para ayudarle a identificar el uso o la propiedad del dominio dentro de su organización.

   Las entradas deben tener un "." incluido en el dominio utilizando el siguiente formato (por ejemplo paloaltonetworks.com), de lo contrario se analiza como un nombre de host, el cual se considera un dominio privado.

3. Haga clic en **OK (Aceptar)** para salir del cuadro de diálogo de configuración del perfil de seguridad antispyware y en **Commit (Confirmar)** para confirmar sus cambios.

STEP 6 | Opcional Configure los ajustes de máximo tiempo de espera de consulta de firma DNS avanzada. Cuando se supera este valor, la respuesta DNS pasa sin realizar el análisis utilizando Advanced DNS Security.

STEP 7 | (Opcional [Si no tiene el certificado del dispositivo más reciente]) Instale un certificado de dispositivo del cortafuegos actualizado utilizado para autenticarse en el servicio de análisis en línea de Advanced Threat Prevention. Repita el procedimiento para todos los cortafuegos habilitados para el análisis en línea de la nube.

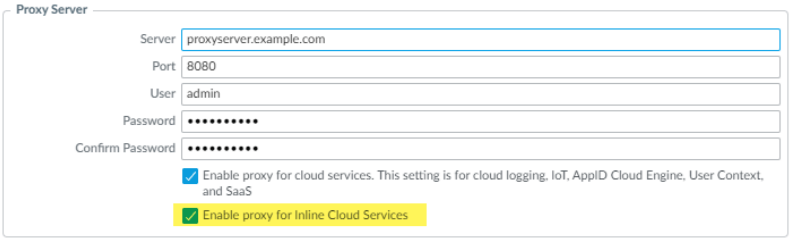
Si ya ha instalado un certificado de dispositivo de cortafuegos actualizado como parte de su proceso de incorporación de IoT Security, Telemetría de dispositivos, Advanced Threat Prevention o Filtrado de URL avanzado, este paso no es necesario.

STEP 8 | (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)**.

STEP 9 | (Opcional) Compruebe el estado de la conectividad de su cortafuegos con el servicio en la nube Advanced DNS Security.

STEP 10 | (Opcional) Supervise la actividad en el cortafuegos para detectar consultas DNS que se hayan detectado mediante Advanced DNS Security. Las categorías de DNS Security analizadas mediante el análisis en tiempo real de Advanced DNS Security del paquete de respuesta DNS tienen el prefijo 'adns' seguido de la categoría. Por ejemplo, adns-dnsmisconfig, donde 'dnsmisconfig' indica el tipo de categoría de DNS compatible. Si la categoría de dominio DNS se determinó analizando el paquete de solicitud DNS, la categoría especificada se muestra con el prefijo «dns» seguido de la categoría. Por ejemplo, «dns-grayware».

1. Acceda a los dominios de prueba de Advanced DNS Security para comprobar que se está aplicando la acción de política para un tipo de amenaza determinado.
2. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)**. Puede filtrar los logs en función del tipo específico de categoría de dominio de Advanced DNS Security, por ejemplo `( category-of-threatid eq adns-hijacking )`, mediante el cual la variable `adns-hijacking` indica consultas DNS que Advanced DNS Security ha categorizado como un intento de secuestro DNS malicioso. Las siguientes categorías de amenazas de Advanced DNS Security disponibles en los logs:

   Categorías de Advanced DNS Security

   - **Secuestro DNS**: `adns-hijacking`

     Los dominios de secuestro de DNS tienen un ID de amenaza de (UTID: 109.004.100).
   - **Configuración errónea de DNS**: `adns-dnsmisconfig`

     los dominios con errores de configuración de DNS tienen tres ID de amenazas, que corresponden a tres variantes de tipos de dominios con errores de configuración de DNS: dnsmisconfig_zone (UTID: 109.004.200), dnsmisconfig_zone_dangling (UTID: 109.004.201), y dnsmisconfig_claimable_nx (UTID: 109,004,202). Puede restringir la búsqueda haciendo referencia cruzada a un valor de ID de amenaza que corresponde a un tipo de dominio de configuración erróea de DNS específico. Por ejemplo, (category-of-threatid eq adns-dnsmisconfig) y (threatid eq 109004200), por el cual 109004200 indica el ID de amenaza de un dominio con configuración errónea de DNS que no enruta tráfico a un dominio activo debido a un problema de configuración del servidor DNS.

   Categorías DNS analizadas mediante el análisis de respuesta mejorado de Advanced DNS Security.

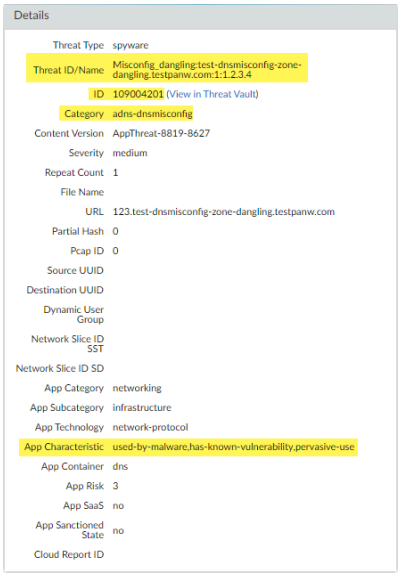
   Debe operar un cortafuegos que ejecute PAN-OS 11.2 y posterior para aprovechar el análisis en tiempo real mejorado de Advanced DNS Security.

   - **DNS** : `adns-benign`
   - **Dominios de malware** : `adns-malware`
   - **Dominios de comando y control**: `adns-c2`
   - **Dominios de phishing**: `adns-phishing`
   - **Dominios alojados en el DNS dinámico**: `adns-ddns`
   - **Dominios recientemente registrados**: `adns-new-domain`
   - **Dominios de Grayware**: `adns-grayware`
   - **Dominios estacionados**: `adns-parked`

- **Evasión de proxy y anonimizadores**: `adns-proxy`
- **Dominios de seguimiento de anuncios**: `adns-adtracking`

Si la consulta DNS no se completa dentro del período de tiempo de espera especificado para Advanced DNS Security, se utilizará la categorización de DNS Security, cuando sea posible. En esos casos, se utiliza la notación heredada para la categoría, por ejemplo, en lugar de `adns-malware`*, se clasificará como* `dns-malware`*, lo que indica que se utilizó el valor de categorización de DNS Security.*

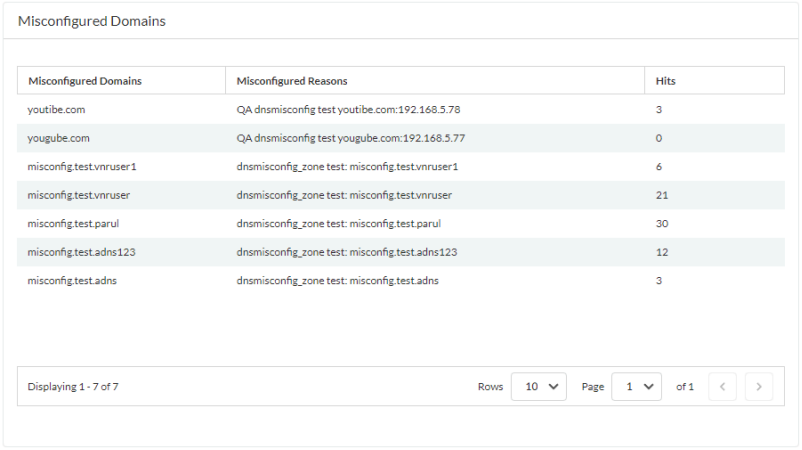
3. Seleccione una entrada de log para ver los detalles de una consulta DNS.
4. La **Category (Categoría)** de DNS se muestra en el panel **Details (Detalles)** de la vista de log detallada. Además, puede ver otros aspectos de la amenaza, incluido el ID de amenaza, que incluye el dominio de origen, la categoría de amenaza específica y otras características asociadas, así como el tipo Q asociado y los datos R con el siguiente formato: secuestro:<FQDN>:<QTYPE>:<RDATA>, mediante el cual <QTYPE> representa el tipo de registro de recursos DNS y <RDATA> representa la dirección IP secuestrada.



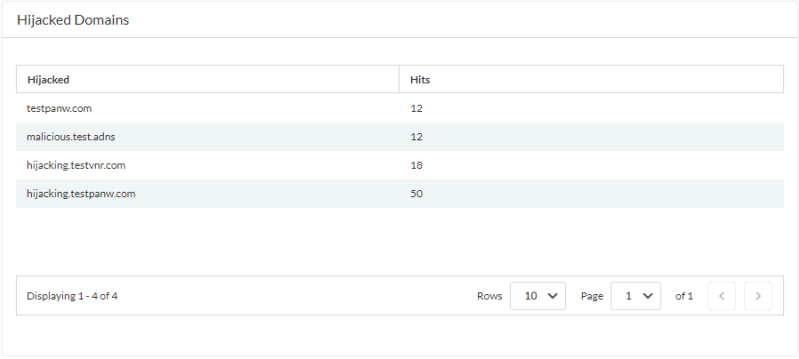
STEP 11 | (Opcional) Recuperar una lista de dominios mal configurados y dominios secuestrados detectados por el servicio de Advanced DNS Security. Los dominios mal configurados se basan en las entradas de dominios principales orientados al público añadidas a **DNS Zone Misconfigurations**.

Las entradas de dominio mal configuradas que se eliminan de la red no se reflejan inmediatamente en las estadísticas del panel de Advanced DNS Security.

1. Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.
2. Seleccione **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **DNS Security** para abrir el panel de DNS Security.
3. Desde el panel de DNS Security, consulte los siguientes widgets:
   - **Misconfigured Domains (Dominios mal configurados)**: vea una lista de dominios que no se pueden resolver asociados con los dominios principales orientados al público especificados por el usuario. Para cada entrada, hay un motivo para la mala configuración y un recuento de resultados de tráfico basado en la IP de origen.



   - **Hijacked Domains (Dominios secuestrados)**: vea una lista de dominios secuestrados determinada por Advanced DNS Security. Para cada entrada, hay un motivo para la clasificación y un recuento de resultados de tráfico basado en la IP de origen.



Configuración de DNS Security sobre 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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Puede obtener visibilidad y control de DNS Security sobre las solicitudes TLS descifrando la carga útil de DNS incluida en la solicitud DNS cifrada. La carga útil del DNS descifrado se puede procesar mediante la configuración del perfil de seguridad que contiene la configuración de políticas DNS. Las solicitudes de DNS que se ha determinado que se originaron en fuentes TLS tienen un puerto de origen de 853 en los logs de amenazas.

- Strata Cloud Manager
- PAN-OS y Panorama

Configuración de DNS Security sobre TLS (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en la aplicación de Strata Cloud Manager en el hub.

STEP 2 | Habilitación de DNS Security está configurado para inspeccionar las solicitudes de DNS. Puede utilizar su perfil de seguridad existente si desea utilizar la misma configuración de **DNS Policies (Políticas DNS)** para DNS Security sobre el tráfico TLS.

STEP 3 | Cree una regla de política de descifrado con una acción para descifrar el tráfico HTTPS en el puerto 853, que incluye DNS Security sobre el tráfico TLS (consulte las Prácticas recomendadas de descifrado para obtener más información). Cuando se descifra DNS Security sobre el tráfico TLS, las solicitudes de DNS resultantes en los logs aparecen como aplicaciones **dns-base** convencionales.

STEP 4 | (Opcional) Busque actividad en el cortafuegos para consultas DNS cifradas con TLS descifradas que se han procesado utilizando DNS Security.

1. Seleccione **Activity (Actividad)** > **Log Viewer (Visor de log)** y seleccione logs de **Threat (Amenazas)**. Utilice el generador de consultas para filtrar en función de la aplicación utilizando **dns-base** y el puerto 853 (que se utiliza exclusivamente para DNS Security sobre transacciones TLS), por ejemplo, `app = 'dns-base' Y source_port = 853`.
2. Seleccione una entrada de log para ver los detalles de la amenaza DNS detectada.

3. La **Application (Aplicación)** deberá mostrar **dns-base** en el panel **General** y el **Port (Puerto)** en el panel **Source (Origen)** de la vista detallada del log. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes pestañas.

Configuración de DNS Security sobre TLS (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Habilitación de DNS Security está configurado para inspeccionar las solicitudes de DNS. Puede utilizar su perfil de seguridad existente si desea utilizar la misma configuración de **DNS Policies (Políticas DNS)** para DNS Security sobre el tráfico TLS.

STEP 3 | Cree una regla de política de descifrado (similar al ejemplo siguiente) con una acción para descifrar el tráfico HTTPS en el puerto 853, que incluye DNS Security sobre el tráfico TLS (consulte las Prácticas recomendadas de descifrado para obtener más información). Cuando se descifra DNS Security sobre el tráfico TLS, las solicitudes de DNS resultantes en los logs aparecen como aplicaciones **dns-base** convencionales.

		Source				Destination					Decrypt Options					
	NAME	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNS SSL HAN
1	Decrypt Port 853	any	any	any	any	any	any	any	any	Port 853	decrypt	ssl-forward-proxy	default	none	false	true

STEP 4 | (Opcional) Busque actividad en el cortafuegos para consultas DNS cifradas con TLS descifradas que se han procesado utilizando DNS Security.

1. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Traffic (Tráfico)** y filtrar en función de la aplicación utilizando **dns-base** y el puerto 853 (que se utiliza exclusivamente para DNS Security sobre transacciones TLS), por ejemplo, `( app eq dns-base ) y ( port.src eq 853 )`.
2. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada.
3. La **Application (Aplicación)** deberá mostrar **dns-base** en el panel **General** y el **Port (Puerto)** en el panel **Source (Origen)** de la vista detallada del log. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.

Configurar DNS Security sobre DoH

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Puede analizar y clasificar la carga útil de DNS contenida en las solicitudes de tráfico DNS cifradas a hosts DNS mediante HTTPS (DoH—[DNS-sobre-HTTPS]). Si su organización actualmente bloquea todas las solicitudes de DoH como recomienda Palo Alto Networks, puede realizar una transición fuera de esa política, ya que DNS Security ahora le permite extraer el nombre de host DNS de la solicitud cifrada y aplicar las políticas de DNS Security existentes de su organización. Esto le permite acceder de forma segura a más sitios web a medida que se amplía el soporte para DoH. El soporte de DNS Security para DoH se habilita mediante la configuración del cortafuegos para descifrar la carga útil de las solicitudes de DNS que se originan en una lista de solucionadores de DNS especificada por el usuario, lo que proporciona soporte para una variedad de opciones de servidor. La carga útil de DNS descifrada se puede procesar mediante la configuración del perfil de antispyware que contiene la configuración de política DNS. Las solicitudes de DNS que se ha determinado que son DoH se etiquetan como **dns-over-https (dns-sobre-https)** en los logs de tráfico.

- Strata Cloud Manager
- (PAN-OS 11.0 y posterior)

Configuración de DNS Security sobre DoH (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

STEP 2 | Crea una lista de categorías de URL personalizadas que incluya todos los solucionadores de DoH para los que quiera habilitar el tráfico (necesitará la URL del servidor DNS).

STEP 3 | Crea una regla de política de descifrado que haga referencia a la lista de categorías de URL personalizadas que se creó en el paso anterior.

STEP 4 | Actualice o cree un nuevo perfil de seguridad antispyware que se utilizará para inspeccionar las solicitudes DoH.

STEP 5 | Cree o actualice una regla de política de seguridad y haga referencia a un perfil de DNS Security y una lista de categorías de URL personalizada [**Manage (Gestionar)** > **Configuration (Configuración)** > **PAN-OS y Prisma Access** > **Security Services (Servicios de seguridad)** > **URL**

Access Management (Gestión de acceso de URL)] que contenga la lista aprobada de servidores DoH.

STEP 6 | Cree una política de bloqueo para descifrar el tráfico HTTPS y bloquee todo el tráfico DoH no autorizado restante que no esté explícitamente permitido por la lista de categorías de URL personalizada (referenciada en el paso 5) mediante el App-ID: **dns-over-https** y la siguiente categoría de URL: **encrypted-dns**.

Si ya tiene una política de bloqueo existente para bloquear el tráfico de DoH, compruebe que la regla se coloca debajo de la regla de política de seguridad anterior utilizada para coincidir con los solucionadores de DoH específicos enumerados en un objeto de lista de categorías de URL personalizado.

STEP 7 | (Opcional) Busque actividad en el cortafuegos para consultas DNS cifradas con HTTPS que se hayan procesado utilizando DNS Security.

1. Seleccione **Activity (Actividad)** > **Logs (Logs)** > **Log Viewer (Visor de logs)** y seleccione **Threat (Amenaza)**.
2. Envíe una consulta de log basada en la aplicación, utilizando **dns-over-https (dns-sobre-https)**, por ejemplo, `app = 'dns-over-https'`.
3. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada que utiliza DoH.
4. La **Application (Aplicación)** de amenazas se muestra en el panel **General** de la vista detallada del log. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.

Configurar DNS Security sobre DoH (PAN-OS 11.0 y posterior)

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

STEP 2 | Crea una lista de categorías de URL personalizadas que incluya todos los solucionadores de DoH para los que quiera habilitar el tráfico (necesitará la URL del servidor DNS).

STEP 3 | Crea una regla de política de descifrado que haga referencia a la lista de categorías de URL personalizadas que se creó en el paso anterior.

STEP 4 | Actualice o cree un nuevo perfil de seguridad antispyware que se utilizará para inspeccionar las solicitudes DoH.

STEP 5 | Cree o actualice una regla de política de seguridad y haga referencia a un perfil antispyware y una lista de categorías de URL personalizada [**Objects (Objetos)** > **Custom Objects (Objetos personalizados)** > **URL Category (Categoría de URL)**] que contienen la lista aprobada de servidores DoH.

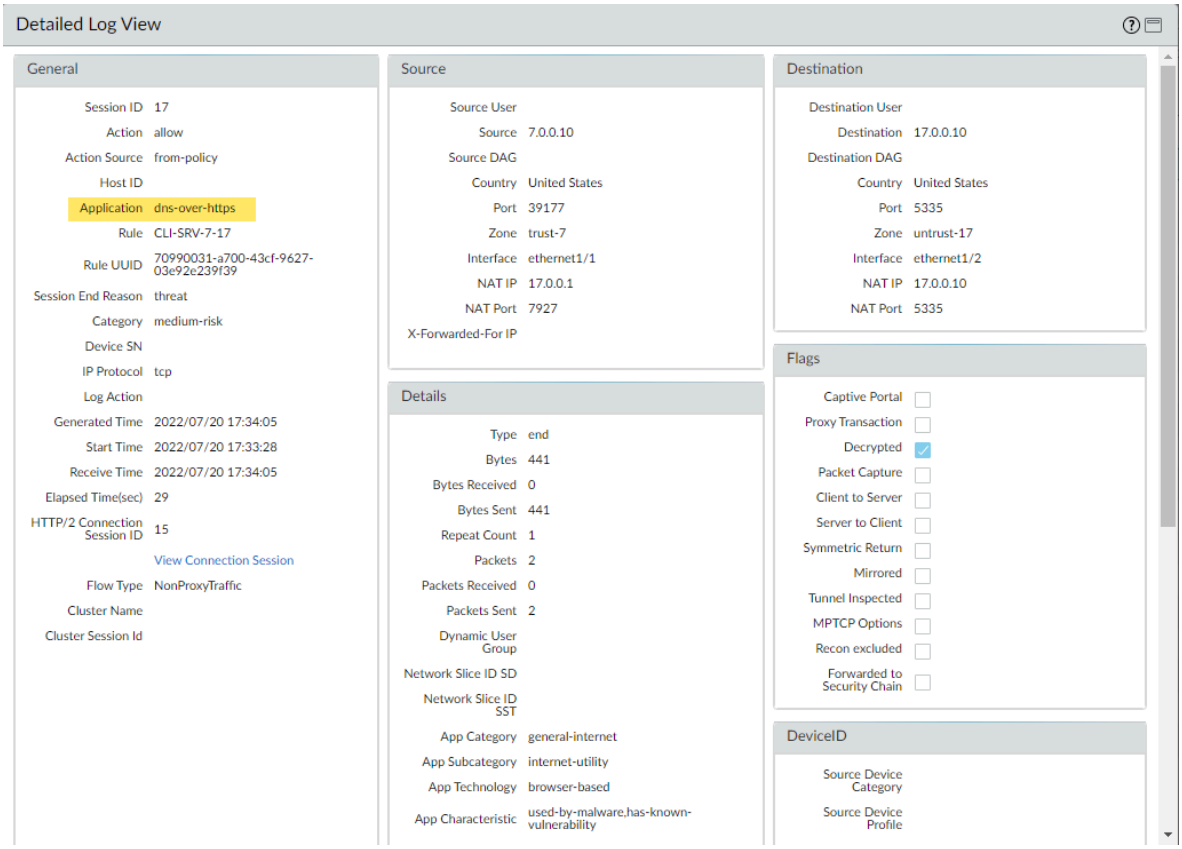
STEP 6 | Cree una política de bloqueo para descifrar el tráfico HTTPS y bloquee todo el tráfico DoH no autorizado restante que no esté explícitamente permitido por la lista de categorías de URL

personalizada (referenciada en el paso 5) mediante el App-ID: **dns-over-https** y la siguiente categoría de URL: **encrypted-dns**.

Si ya tiene una política de bloqueo existente para bloquear el tráfico de DoH, compruebe que la regla se coloca debajo de la regla de política de seguridad anterior utilizada para coincidir con los solucionadores de DoH específicos enumerados en un objeto de lista de categorías de URL personalizado.

STEP 7 | (Opcional) Busque actividad en el cortafuegos para consultas DNS cifradas con HTTPS que se hayan procesado utilizando DNS Security.

1. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Traffic (Tráfico)** y filtre en base a la aplicación mediante **dns-over-https (dns-sobre-https)**, por ejemplo, `( app eq dns-over-https )`.
2. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada.
3. La **Application (Aplicación)** debe mostrar dns-over-https en el panel **General (General)** de la vista de log detallada, indicando que se trata de tráfico DoH que se ha procesado utilizando DNS Security. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.



Crear excepciones de dominio y listas de permitidos | bloqueados

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

DNS Security crea firmas de amenazas para los dominios que el servicio de DNS Security ha analizado. Para estos dominios conocidos, se hace referencia a las firmas cuando se recibe una consulta DNS. En algunos casos, es posible que la firma haya clasificado incorrectamente un dominio como una amenaza, debido a ciertas características o cualidades presentes en el dominio. En tales circunstancias, puede añadir excepciones de firma para evitar estos falsos positivos. Si hay dominios seguros conocidos que se clasifican como malintencionados, como dominios internos, puede añadir una lista de dominios que omitirán cualquier análisis de DNS. Si su organización utiliza fuentes de amenazas de terceros como parte de una solución integral de inteligencia sobre amenazas, también puede hacer referencia a ellas en forma de listas dinámicas externas (EDL) en su perfil de DNS Security.

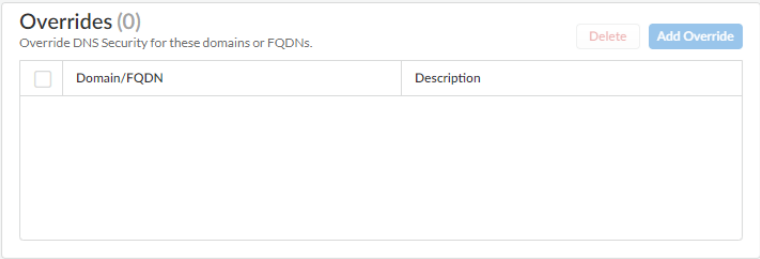
- Strata Cloud Manager
- PAN-OS y Panorama

Crear excepciones de dominio y listas de permitidos | bloqueados (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

STEP 2 | Añada anulaciones de dominio en los casos donde se produzcan falsos positivos.

1. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access** > **Security Services (Servicios de seguridad)** > **DNS Security** y seleccione un perfil de DNS Security para modificar.
2. Debe **Add Override (Añadir anulación)** o **Delete (Eliminar)** para modificar las entradas de la lista de dominios según sea necesario. Cada entrada adicional requiere el dominio y una descripción.



3. Haga clic en **OK (Aceptar)** para guardar su perfil de DNS Security modificado.

STEP 3 | Haga referencia a una lista dinámica externa (EDL) como parte de su perfil de DNS Security para importar fuentes de amenazas de terceros.

1. Cree una lista dinámica externa basada en dominios [**Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW and (NGFW y) Prisma Access** > **Objects (Objetos)** > **External Dynamic Lists (Listas dinámicas externas)**]. Para obtener más información sobre las EDL, consulte External Dynamic Lists (Lista dinámica externa).
2. Seleccione **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access** > **Security Services (Servicios de Seguridad)** > **Security Services**.
3. En el panel **External Dynamic Lists (Listas dinámicas externas)**, seleccione una lista de dominios EDL y proporcione las configuraciones **Policy Action (Acción de política)** y **Packet Capture (Captura de paquetes)**. En **Apply to Profiles (Aplicar a perfiles)**, seleccione el perfil de DNS Security al que desea que se aplique la lista de dominios EDL.
4. Elija **Save (Guardar)** para guardar los cambios cuando haya terminado de realizar las actualizaciones.

Crear excepciones de dominio y listas de permitidos | bloqueados (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 y versiones posteriores proporcionan una opción adicional para añadir explícitamente dominios permitidos a través del perfil de seguridad antispyware. Puede añadir entradas de dominio/FQDN para fuentes de dominio aprobados si desencadenan una respuesta falsa positiva de DNS Security.

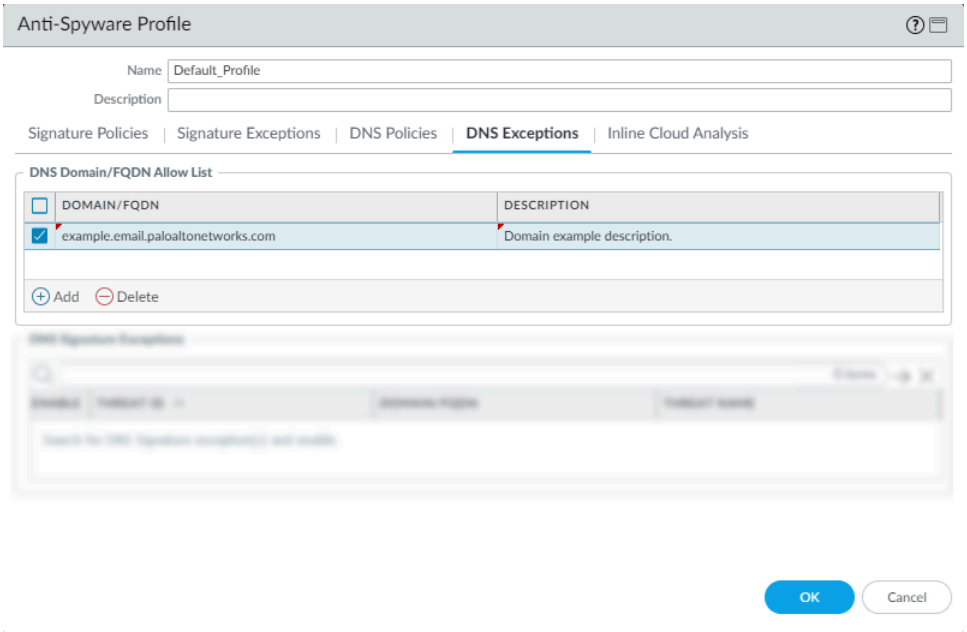
- PAN-OS 10.0.x y posterior
- PAN-OS 9.1

Crear excepciones de dominio y listas de permitidos | bloqueados (PAN-OS 10.0 y versiones posteriores)

- Inicie sesión en el NGFW.

- Añada excepciones de firma de dominio en los casos en los que se produzcan falsos positivos.
  1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
  2. Seleccione el perfil que desea modificar.
  3. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antispyware o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **DNS Exceptions (Excepciones de DNS)**.
  4. Introduzca el nombre o el FQDN de la firma de DNS que se debe excluir para buscarla.
  5. Active la casilla de verificación para cada **Threat ID (ID de amenaza)** cuya firma desea excluir del proceso de aplicación.
  6. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

- Agregue una lista de permitidos para especificar una lista de dominios DNS o FQDN que se permitirán de forma explícita.
  1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
  2. Seleccione el perfil que desea modificar.
  3. Haga clic en **Add (Añadir)** para añadir un nuevo perfil de antispyware o modifique uno existente en el que desea excluir una firma de amenazas, y seleccione **DNS Exceptions (Excepciones de DNS)**.
  4. Para **Add (Añadir)** una nueva entrada de la lista de permitidos de FQDN, proporcione el dominio DNS o la ubicación del FQDN y una descripción.



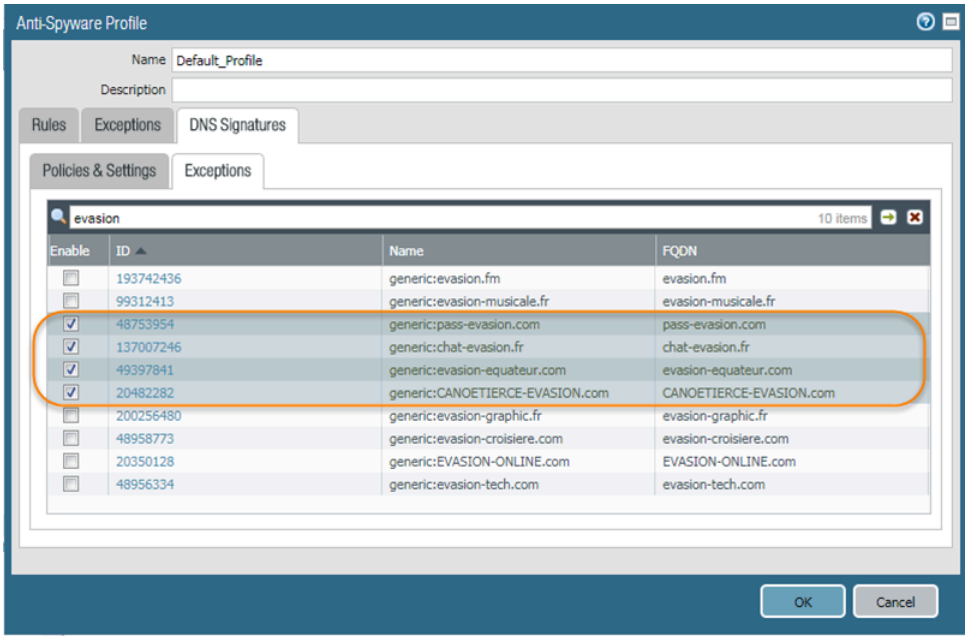
  5. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

Crear excepciones de dominio y listas de permitidos | bloqueados (PAN-OS 9.1)

Las listas de permitidos y bloqueados no están disponibles en PAN-OS 9.1.

- Inicie sesión en el NGFW.

- Añada excepciones de firma de dominio en los casos en los que se produzcan falsos positivos.
  1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
  2. Seleccione el perfil que desea modificar.
  3. Haga clic en **Add (Añadir)** para añadir el perfil de antispyware del que desea excluir la firma contra amenazas o modifique uno existente y seleccione **DNS Signatures (Firmas de DNS)** > **Exceptions (Excepciones)**.
  4. Introduzca el nombre o el FQDN de la firma de DNS que se debe excluir para buscarla.
  5. Marque la casilla **DNS Threat ID (ID de la amenaza de DNS)** cuya firma desea excluir del proceso de aplicación.



  6. Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware modificado o uno nuevo.

Dominios de prueba

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Palo Alto Networks proporciona los siguientes dominios de prueba de DNS Security para validar su configuración de política en base a la categoría de DNS.

STEP 1 | Acceda a los siguientes dominios de prueba para comprobar que se está aplicando la acción de política para un tipo de amenaza determinado:

DNS Security

- C2: test-c2.testpanw.com
- DNS Tunneling (Tunelización de DNS): test-dnstun.testpanw.com
- DGA: test-dga.testpanw.com
- DNS dinámico*: test-ddns.testpanw.com
- Malware: test-malware.testpanw.com
- Dominios registrados recientemente*: test-nrd.testpanw.com
- Phishing*: test-phishing.testpanw.com
- Grayware*: test-grayware.testpanw.com
- Estacionado*: test-parked.testpanw.com
- Evasión de proxy y anonimizadores*: test-proxy.testpanw.com
- Fast Flux*: test-fastflux.testpanw.com
- NRD malintencionado*: test-malicious-nrd.testpanw.com
- NXNS Attack*: test-nxns.testpanw.com
- Colgante*: test-dangling-domain.testpanw.com
- Revinculación de DNS*: test-dns-rebinding.testpanw.com
- Infiltración de DNS*: test-dns-infiltration.testpanw.com
- Abuso de comodines*: test-wildcard-abuse.testpanw.com
- Estratégicamente envejecidos*: test-strategically-aged.testpanw.com
- DNS comprometido*: test-compromised-dns.testpanw.com
- Seguimiento de anuncios*: test-adtracking.testpanw.com
- Encubrimiento CNAME*:test-cname-cloaking.testpanw.com
- Ransomware*: test-ransomware.testpanw.com
- Stockpile*—test-stockpile-domain.testpanw.com
- Ciberocupación*: test-squatting.testpanw.com
- Reputación del subdominio*: test-subdomain-reputation.testpanw.com

*Los dominios de prueba marcados con un * no son compatibles con PAN-OS 9.1.*

Advanced DNS Security

Acceda al siguiente dominio de prueba para comprobar que se está aplicando la acción de política para un tipo de amenaza determinado:

- **Dominio con error de configuración** DNS (reclamable): http://test-dnsmisconfig-claimable-nx.testpanw.com

Los siguientes casos de prueba de dominio de prueba se deben añadir al archivo de zona del servidor DNS de testpanw.com antes de acceder al dominio. Estos casos de prueba coinciden con las firmas de Advanced DNS Security y generarán los logs apropiados. Compruebe que la acción de política para un tipo de amenaza determinado se está aplicando.

Table 1: Casos de prueba de dominio con errores de configuración de DNS (Zona Dangling)

Host	Tipo de registro	Datos de registro
*.test-dnsmisconfig-zone-dangling.testpanw.com	A	1.2.3.4

Table 2: Casos de prueba de dominio de secuestro

Host	Tipo de registro	Datos de registro
test-ipv4.hijacking.testpanw.com	A	1.2.3.5
*.test-ipv4-wildcard.hijacking.testpanw.com	A	1.2.3.6
test-ipv6.hijacking.testpanw.com	AAAA	2607:f8b0:4005:80d::2005
test-cname-rrname.hijacking.testpanw.com	CNAME	1.test-cname-wc.hijacking.testpanw.com
test-cname-rrname-wc.hijacking.testpanw.com	CNAME	1.test-cname-wildcard-1.hijacking.testpanw.com
*.test-cname-rrname-sub-wc.hijacking.testpanw.com	CNAME	2.test-cname-wc.hijacking.testpanw.com
test-ns-rrname.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-ns-rrname-rdata-wc.hijacking.testpanw.com	NS	1.test-ns-wc.hijacking.testpanw.com
1.test-ns-rrname-sub-wc.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-rrname-wc.hijacking.testpanw.com	NS	test-ns-2.hijacking.testpanw.com

*Para registros NS, debe usar la siguiente opción:"**dig +trace NS**"*

STEP 2 | Compruebe que DNS Security ha procesado la solicitud de consulta DNS mediante la supervisión de la actividad.

Prueba de conectividad a los servicios de nube de DNS Security

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

DNS Security

Verifique la conectividad de su cortafuegos con el servicio de DNS Security. Si no puede comunicarse con el servicio, verifique que el siguiente dominio no esté bloqueado: dns.service.paloaltonetworks.com.

STEP 1 | Acceda a la CLI del cortafuegos.

STEP 2 | Utilice el siguiente comando de la CLI para verificar la disponibilidad de conexión de su cortafuegos con el servicio de seguridad DNS.

```
show dns-proxy dns-signature info
```

Por ejemplo:

```
show dns-proxy dns-signture info Cloud URL:
 dns.service.paloaltonetworks.com:443 Telemetry URL:
 io.dns.service.paloaltonetworks.com:443 Last Result: None Last
 Server Address: Parameter Exchange: Interval 300 sec Allow List
 Refresh: Interval 43200 sec Request Waiting Transmission: 0
 Request Pending Response: 0 Cache Size: 0
```

Si el cortafuegos tiene una conexión activa al servicio de DNS security, los detalles del servidor se muestran en el resultado de respuesta.

STEP 3 | Recupere los detalles de la transacción de un dominio específico, como la latencia, TTL y la categoría de firma.

Use el siguiente comando de la CLI en el cortafuegos para revisar los detalles del dominio:

```
test dns-proxy dns-signature fqdn
```

Por ejemplo:

```
test dns-proxy dns-signature fqdn www.yahoo.com DNS
 Signature Query [ www.yahoo.com ] Completed in 178 ms DNS
```

```
 Signature Response Entries: 2 Domain Category GTID TTL
 ------------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

Advanced DNS Security

Verifique la conectividad de su cortafuegos con el servicio de Advanced DNS Security. Si no puede comunicarse con el servicio, verifique que el siguiente dominio no esté bloqueado: adv-dns.service.paloaltonetworks.com Si ha configurado manualmente un servidor regional de Advanced DNS Security, es posible que deba verificar que el dominio regional específico también está desbloqueado.

Compruebe el estado de la conectividad de su cortafuegos con el servicio en la nube Advanced DNS Security.

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 ADNS(1)
 Current cloud server: qa.adv-dns.service.paloaltonetworks.com:443
 Cloud connection: connected Config: Number of gRPC connections:
 2, Number of workers: 8 Debug level: 2, Insecure connection:
 false, Cert valid: true, Key valid: true, CA count: 306 Maximum
 number of workers: 12 Maximum number of sessions a worker should
 process before reconnect: 10240 Maximum number of messages
 per worker: 0 Skip cert verify: false Grpc Connection Status:
 State Ready (3), last err rpc error: code = Unavailable desc
 = unexpected HTTP status code received from server: 502 (Bad
 Gateway); transport: received unexpected content-type "text/html"
 Pool state: Ready (2) last update: 2024-01-24 11:15:00.549591469
 -0800 PST m=+1197474.129493596 last connection retry: 2024-01-23
 00:03:09.093756623 -0800 PST m=+1070762.673658768 last pool
 close: 2024-01-22 14:15:50.36062031 -0800 PST m=+1035523.940522446
 Security Client AdnsTelemetry(2) Current cloud server: io-qa.adv-
dns.service.paloaltonetworks.com:443 Cloud connection: connected
 Config: Number of gRPC connections: 2, Number of workers: 8 Debug
 level: 2, Insecure connection: false, Cert valid: true, Key
 valid: true, CA count: 306 Maximum number of workers: 12 Maximum
 number of sessions a worker should process before reconnect:
 10240 Maximum number of messages per worker: 0 Skip cert verify:
 false Grpc Connection Status: State Ready (3), last err rpc error:
 code = Internal desc = stream terminated by RST_STREAM with error
 code: PROTOCOL_ERROR Pool state: Ready (2) last update: 2024-01-24
 11:25:58.340198656 -0800 PST m=+1198131.920100772 last connection
 retry: 2024-01-23 00:03:36.78141425 -0800 PST m=+1070790.361316421
 last pool close: 2024-01-22 14:24:26.954340157 -0800 PST m=
+1036040.534242289 ...
```

Compruebe que el estado de la conexión en la nube de `Security Client AdnsTelemetry(2)` y `Security Client ADNS(1)` muestra conexiones activas.

Resultado de CLI acortado por brevedad.

Si no puede conectarse al servicio en la nube de Advanced DNS Security, compruebe que el servidor DNS avanzado no esté bloqueado: dns.service.paloaltonetworks.com.

Configurar tiempo de espera de búsqueda

¿Dónde puedo usar esto?	¿Qué necesito?
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

DNS Security

Si el cortafuegos no puede recuperar un veredicto de firma en el tiempo asignado debido a problemas de conectividad, se pasa la solicitud, incluidas todas las respuestas DNS posteriores. Puede verificar la latencia media para comprobar que las solicitudes se encuentren dentro del periodo configurado. Si la latencia media supera el periodo configurado, considere actualizar la configuración a un valor que sea superior a la latencia media para evitar que el tiempo de espera de las solicitudes se agote.

STEP 1 | En la CLI, emita el siguiente comando para ver la latencia media.

```
show dns-proxy dns-signature counters
```

El tiempo de espera predeterminado es de 100 milisegundos.

STEP 2 | Desplácese hacia abajo a través del resultado hasta la sección de latencia en el encabezado de la API de consulta de firma y compruebe que la latencia media se encuentre dentro del periodo de espera definido. Esta latencia indica la cantidad de tiempo que tarda, de media, en recuperar un veredicto de firma del servicio de seguridad de DNS. Puede encontrar estadísticas de latencia adicionales para varios periodos de latencia inferiores a las medias.

```
Signature query API: . . . [latency ] : max 1870 (ms) min 16(ms)
 avg 27(ms) 50 or less : 47246 100 or less : 113 200 or less : 25
 400 or less : 15 else : 21
```

STEP 3 | Si la latencia media está coherentemente por encima del valor de tiempo de espera predeterminado, puede aumentar la configuración para que las solicitudes se encuentren dentro de un periodo determinado. Seleccione **Device (Dispositivo) > Content-ID** y actualice la configuración de **Realtime Signature Lookup (Consulta de firma en tiempo real)**.

STEP 4 | Confirme los cambios.

Advanced DNS Security

STEP 1 | Vea el registro de los tiempos de ida y vuelta (en milisegundos) de las solicitudes de Advanced DNS Security mediante el siguiente comando de depuración de la CLI. Estos se distribuyen en soportes de

latencia de 0 ms a 450 ms. Puede usar esto para determinar la configuración de latencia máxima ideal para su NGFW.

```
admin@PA-VM debug dataplane show ctd feature-forward stats
```

En la salida de respuesta, vaya a la sección `PAN_CTDF_DETECT_SERVICE_ADNS`.

```
PAN_CTDF_DETECT_SERVICE_ADNS cli_timeout: 1 req_total: 2
 req_timed_out: 0 Hold: adns rtt>=0ms: 0 adns rtt>=50ms: 2
 adns rtt>=100ms: 0 adns rtt>=150ms: 0 adns rtt>=200ms: 0
 adns rtt>=250ms: 0 adns rtt>=300ms: 0 adns rtt>=350ms: 0 adns
 rtt>=400ms: 0 adns rtt>=450ms: 0
```

STEP 2 | Configure los ajustes de máximo tiempo de espera de consulta de firma DNS avanzada. Cuando se supera este valor, la respuesta DNS pasa sin realizar el análisis utilizando Advanced DNS Security. Las firmas DNS (y sus políticas asociadas) que se entregan a través de actualizaciones de contenido regulares o forman parte de las EDL (listas dinámicas externas) configuradas o excepciones DNS todavía se aplican.

1. Seleccione **Device (Dispositivo)** > **Setup (Configuración)** > **Content-ID** > **Advanced DNS Security**.
2. Especifique un ajuste de máximo tiempo de espera de consulta de firma DNS avanzada actualizada en milisegundos. El valor predeterminado es 100 ms y esa es la configuración recomendada.
3. Haga clic en **OK (Aceptar)** para confirmar los cambios.

De forma alternativa, puede utilizar el siguiente comando de la CLI para configurar el valor de tiempo de espera de Advanced DNS Security. Puede establecer un valor de 100 - 15.000 ms en incrementos de 100 ms. El valor predeterminado es 100 ms y esa es la configuración recomendada.

```
admin@PA-VM#set deviceconfig setting adns-setting max-latency
 <timeout_value_in_milliseconds>
```

Por ejemplo:

```
admin@PA-VM# set deviceconfig setting adns-setting max-latency 500
```

Puede comprobar la configuración de tiempo de espera actual mediante el siguiente comando de la CLI (consulte la entrada **`max-latency`** del resultado).

```
admin@PA-VM show config pushed-template ... }
 deviceconfig { setting { dns { dns-cloud-server dns-
qa.service.paloaltonetworks.com; } adns-setting { max-latency
 100; } } } ...
```


Omitir Servicios de suscripciones de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Las consultas de DNS Security se pueden omitir en los casos en los que hay problemas de latencia u otros problemas de red.

En los casos en los que se producen falsos positivos, Palo Alto Networks recomienda crear excepciones específicas en lugar de omitir las consultas de DNS Security.

- Gestión de la nube
- PAN-OS y Panorama

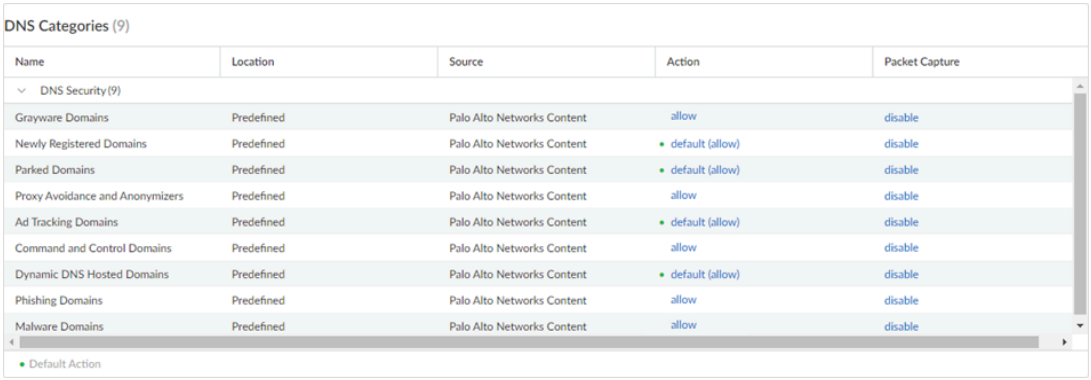
Omitir Servicios de suscripciones de DNS Security (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

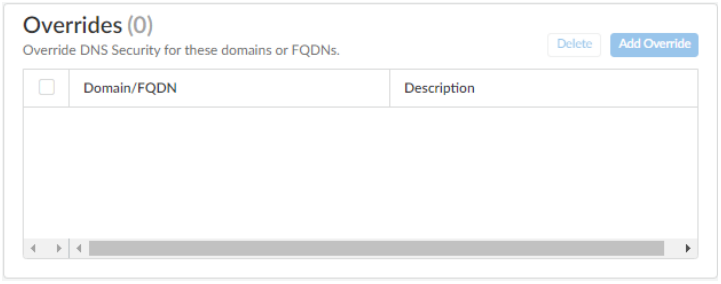
STEP 2 | Vaya a **Manage (Gestionar)** > **Configuration (Configuración)** > **NGFW y Prisma Access** > **Security Services (Servicios de seguridad)** > **DNS Security** y seleccione el perfil de DNS Security relevante.

STEP 3 | Configure la configuración de las políticas de firma de DNS Security para omitir las consultas de DNS Security. Para cada categoría de DNS, configure la **Action (Acción)** en **allow (permitir)** y la

Packet Capture (Captura de paquetes) en **disabled (deshabilitada)**. A continuación, las categorías de DNS Security se han configurado para omitir las consultas de DNS Security.



STEP 4 | En la sección **Overrides (Anulaciones)**, verifique que no haya entradas presentes; si es necesario, elimine todas las anulaciones de **Domain/FQDN (Dominio/FQDN)**.



STEP 5 | Haga clic en **OK (Aceptar)** para guardar el perfil de DNS Security.

Omitir Servicios de suscripciones de DNS Security (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 y versiones posteriores son compatibles con fuentes de firma DNS configurables individualmente, lo que le permite definir acciones de políticas independientes, así como un nivel de gravedad de logs para un origen de firma determinado. Esto requiere que configure tanto la acción de la política como la gravedad de logs para cada fuente de firma DNS disponible para omitir DNS Security. Además, también debe eliminar las entradas de excepciones de DNS para que DNS Security se omita por completo. En PAN-OS 9.1, puede simplemente establecer la acción de política para DNS Security de Palo Alto Networks en una acción de permitir.

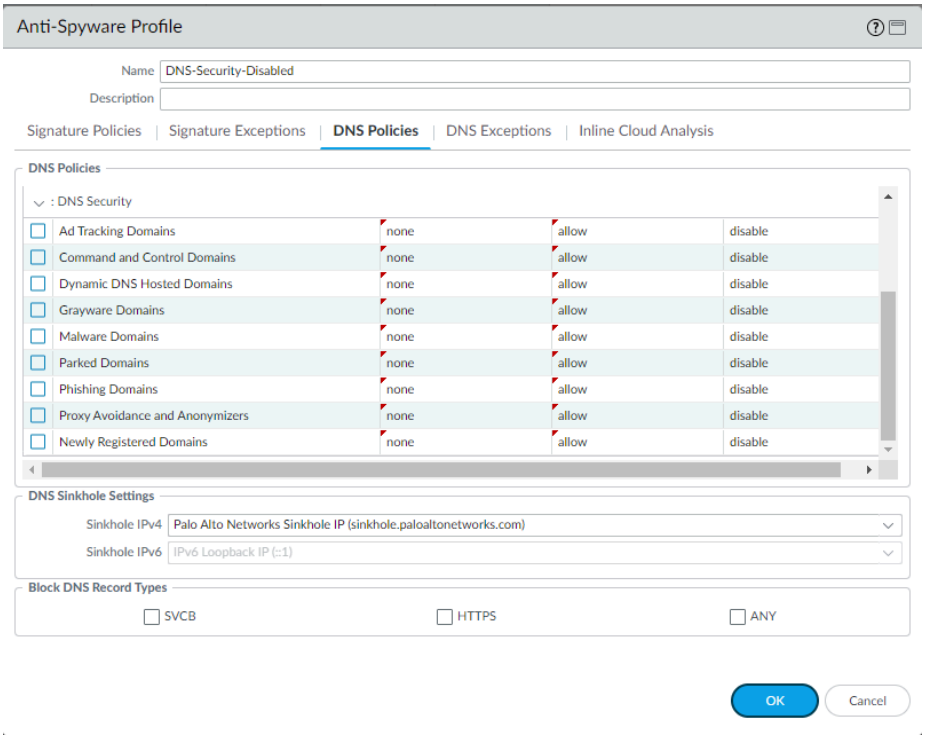
- PAN-OS 10.0.x y posterior
- PAN-OS 9.1

Omitir Servicios de suscripción de DNS Security (PAN-OS 10.0 y posterior)

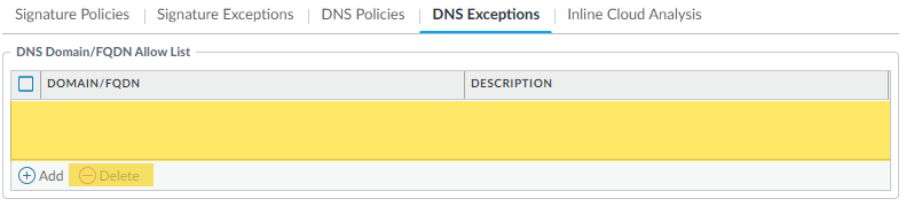
STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Configure la configuración de las políticas de firma de DNS Security para omitir las consultas de DNS Security.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Seleccione el perfil que contiene la configuración activa de políticas de DNS Security.
3. Seleccione la pestaña **DNS Policies (Políticas DNS)**.
4. Para cada categoría de DNS, establezca la gravedad de logs en **none (ninguna)**, la acción de política en **allow (permitir)** y la captura de paquetes en **disable (deshabilitar)**. A continuación, las categorías de DNS Security se han configurado para omitir las consultas de DNS Security.



STEP 3 | Seleccione **DNS Exceptions (Excepciones DNS)** y elimine todas las entradas de **DNS Domain/FQDN Allow List (Dominio DNS/Lista de permitidos de FQDN)**.



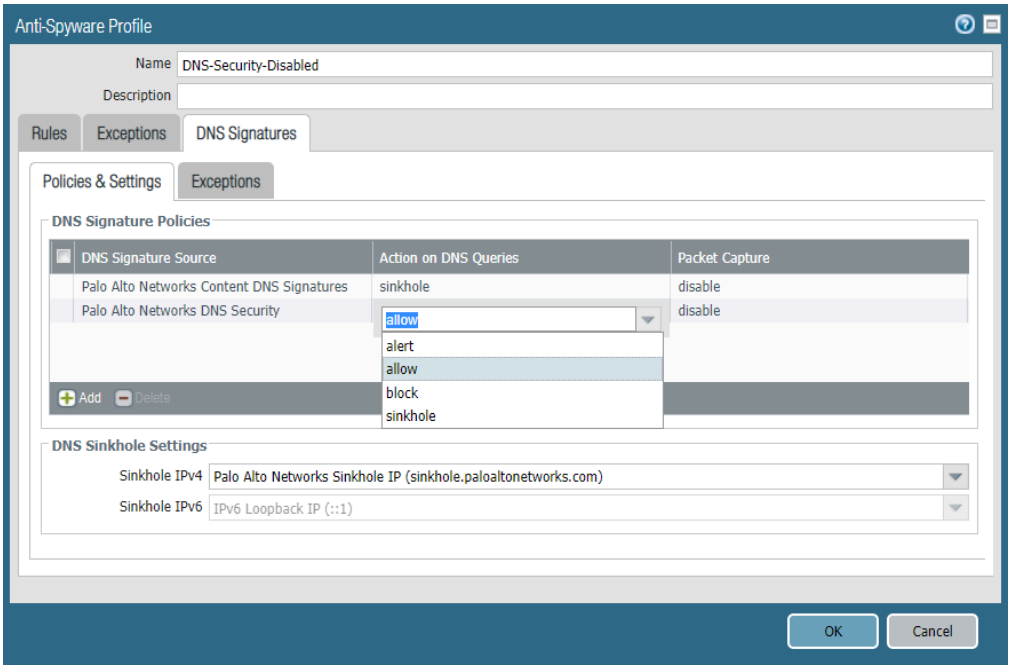
STEP 4 | Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

Omitir Servicios de suscripciones de DNS Security (PAN-OS 9.1)

STEP 1 | Inicie sesión en el NGFW.

STEP 2 | Configure la configuración de las políticas de firma de DNS Security para omitir las consultas de DNS Security.

1. Seleccione **Objects (Objetos)** > **Security Profiles (Perfiles de seguridad)** > **Anti-Spyware**.
2. Seleccione el perfil que contiene la configuración activa de políticas de DNS Security.
3. Seleccione la pestaña **DNS Signatures (Firmas DNS)**.
4. En **Policies & Settings (Políticas y configuración)**, establezca la acción de política para **Palo Alto Networks DNS Security (DNS Security de Palo Alto Networks)** como una acción de **allow (permitir)**.



STEP 3 | Haga clic en **OK (Aceptar)** para guardar el perfil de antispyware.

Supervise los servicios de suscripción de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Palo Alto Networks ofrece varias opciones para supervisar la actividad de DNS Security y Advanced DNS Security para acomodar la recuperación de inteligencia para una gama de productos que dependen de los servicios de suscripción de DNS Security y los datos de tráfico asociados. Dependiendo de la plataforma del producto, puede acceder a paneles de alto nivel que proporcionan estadísticas de solicitudes de DNS y tendencias de uso, incluido contexto sobre la actividad de red, detalles específicos de solicitudes de DNS de usuarios específicos en forma de datos de creación de logs.

También puede ver cómo se integran los servicios de suscripción de DNS Security con otras aplicaciones y servicios de seguridad de Palo Alto Networks para proteger a su organización frente a amenazas, así como obtener una vista de alto nivel del estado operativo general de su implementación, a través del Centro de control de Strata Cloud Manager. El centro de comandos funciona como su página de inicio de NetSec y proporciona un resumen completo de la salud, la seguridad y la eficacia de su red, en un panel visual interactivo con múltiples facetas de datos para una evaluación fácil y rápida.

Para obtener detalles más específicos sobre las operaciones del servicio de suscripción de DNS Security, el panel de control proporciona una vista de sus redes de datos de consulta DNS, así como la capacidad de profundizar en varias tendencias DNS. Cada tarjeta de panel proporciona una vista única de cómo se procesan y clasifican las solicitudes y respuestas DNS en un formato de informe gráfico. Esto le permite ver, de un vistazo, una vista de alto nivel de las estadísticas de uso de DNS de su organización. También proporciona una lista de dominios mal configurados y dominios secuestrados detectados por el servicio de Advanced DNS Security, lo que le permite corregir y rectificar cualquier error de configuración DNS. Los dominios mal configurados se basan en las entradas de dominios principales orientados al público añadidas a la lista **DNS Zone Misconfigurations (Configuraciones erróneas de la zona DNS)**.

También puede ver los logs que se generan automáticamente cuando se procesan las solicitudes de DNS. Estos archivos de eventos tienen una marca de tiempo y proporcionan una pista de auditoría cuando se configuran para hacerlo, según la configuración del log de categoría de DNS. Las entradas de registros DNS pueden contener varios detalles sobre la solicitud DNS, incluida la naturaleza de la amenaza DNS que representa el dominio asociado, así como las acciones realizadas cuando se detectó la amenaza.

Palo Alto Networks proporciona varios métodos para supervisar la actividad de DNS Security en función de su plataforma.

- El Centro de comandos de Strata Cloud Manager
- Ver panel de DNS Security
- Ver logs de DNS Security para las consultas DNS que pasaron por mi red

Ver panel de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

El panel de DNS Security muestra los datos estadísticos generados por los servicios de suscripción de Advanced DNS Security y DNS Security en un informe de evaluación visual y rápida del uso de DNS de su organización. Vea y profundice sobre varias tendencias de DNS descubiertas en su red. Cada tarjeta de panel proporciona una vista única de cómo se procesan y clasifican las solicitudes de DNS. Seleccione tarjetas de panel para cambiar el contexto del panel o ver más información sobre una tendencia, dominio o estadística específicos.

El panel de DNS Security está disponible en Prisma Access y AIOps para NGFW. Puede interactuar con el Tarjetas de panel de DNS Security para modificar el contexto del panel o ver más información sobre una tendencia, dominio o estadística específicos. También puede personalizar el formato para mostrar tendencias actuales o datos históricos en todos los puntos de datos relevantes.

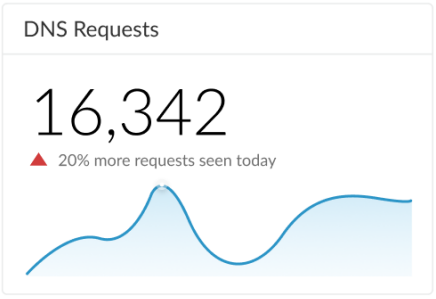
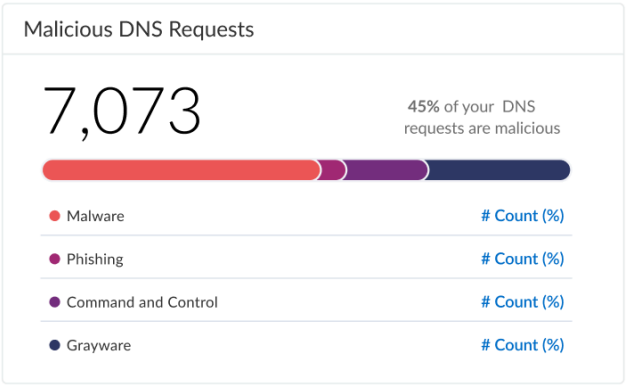
- Strata Cloud Manager
- AIOps para NGFW gratuita

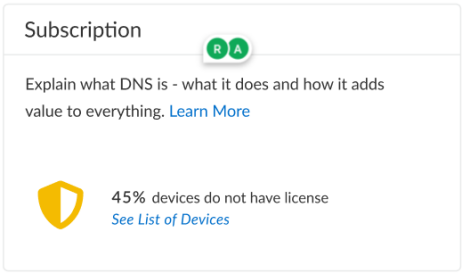
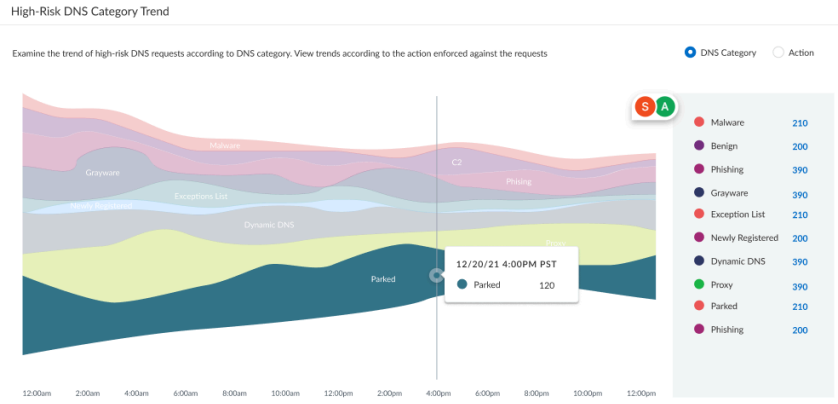
Tarjetas de panel de DNS Security

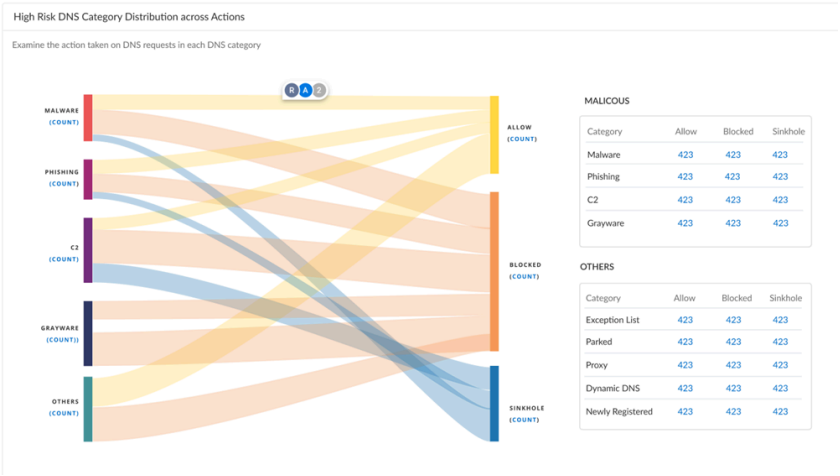
¿Dónde puedo usar esto?	¿Qué necesito?
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

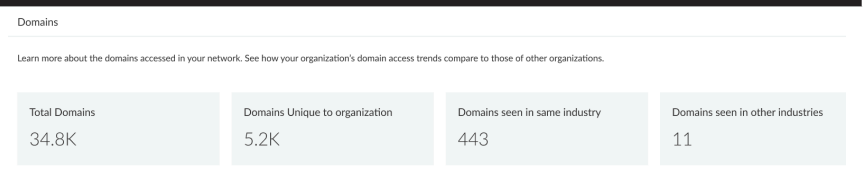
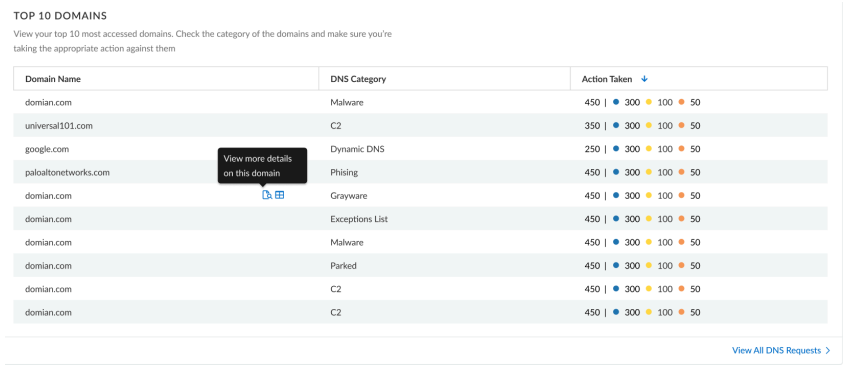
Las tarjetas que completan el panel de DNS Security son interactivas y le permiten ver detalles adicionales o acceder a una lista de solicitudes, eventos y dominios específicos, en lo que respecta a cómo se muestra el contenido.

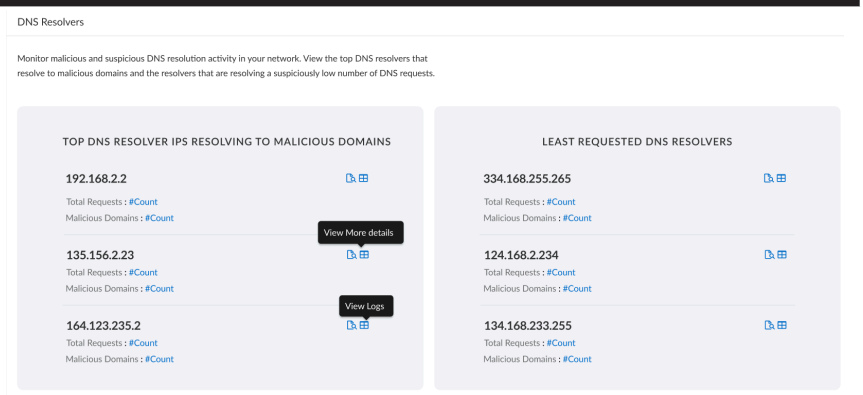
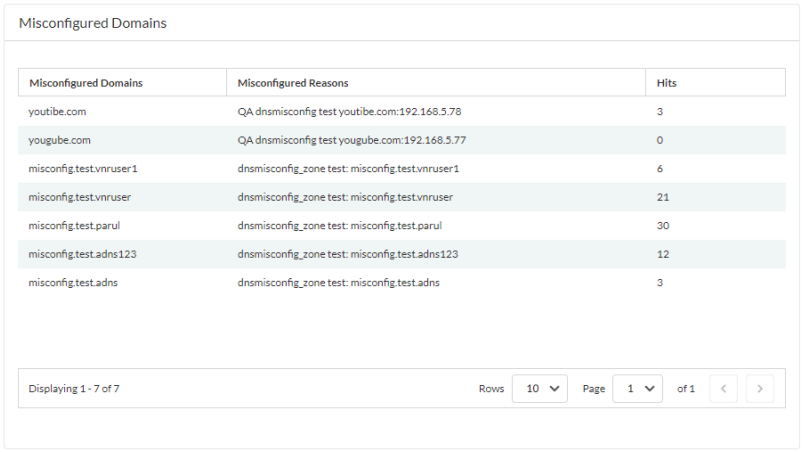
La siguiente lista proporciona una descripción general de las tarjetas del panel de DNS Security:

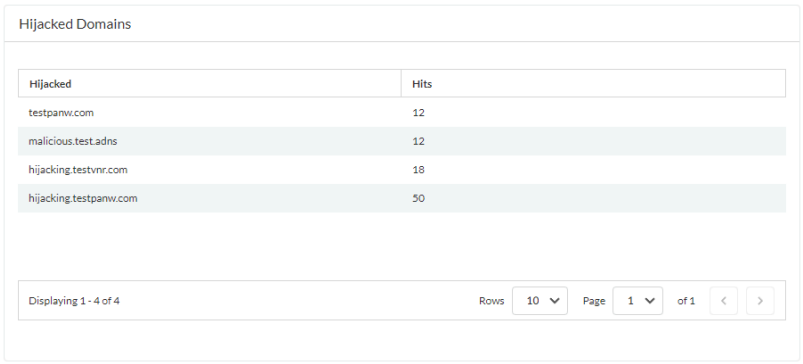
Nombre de la tarjeta	Descripción
Solicitudes de DNS	Muestra el número total de solicitudes de DNS que ha procesado DNS Security.  • El gráfico de líneas dibuja el número de solicitudes de DNS según el rango de tiempo definido por el usuario. Al especificar un rango de tiempo personalizado, el gráfico de líneas se actualiza en consecuencia. • Los filtros de categoría y acción DNS no alteran el contenido de la tarjeta.
Solicitudes de DNS maliciosas	Muestra un gráfico de barras apiladas que muestra las solicitudes de DNS que se han clasificado según los tipos actualmente disponibles que se consideran maliciosos. El número total se muestra en la parte superior izquierda, mientras que un desglose de las variables categóricas se indica a continuación.  • El gráfico de líneas dibuja el número de solicitudes de DNS según el rango de tiempo definido por el usuario. Al especificar un rango de tiempo personalizado, el gráfico de líneas se actualiza en consecuencia. • Los filtros de categoría y acción DNS no alteran el contenido de la tarjeta.

Nombre de la tarjeta	Descripción
Suscripción	Muestra el número de dispositivos en su red con una suscripción de DNS Security activa. También se muestra, con un enlace a una lista completa, un porcentaje de dispositivos que no están equipados con DNS Security o tienen una suscripción caducada.  • Puede seleccionar **See a List of Devices (Ver una lista de dispositivos)** para ver una lista completa. • Esta tarjeta muestra una instantánea del estado actual de la suscripción; las opciones de filtro no tienen ningún impacto.
Tendencia de categorías DNS de alto riesgo	Muestra un gráfico de tendencias que muestra un desglose de las solicitudes de DNS según la categoría de DNS o la acción aplicada a la solicitud de DNS durante el rango de tiempo de observación.  • Seleccione entre un gráfico de categoría de DNS o tendencia de acción utilizando el botón de opción. • Coloque el cursor sobre un segmento en el gráfico de flujo que representa un tipo de datos para aislarlo y abrir una ventana emergente que muestra el número de solicitudes de DNS o el tipo de acción realizada. • Cuando especifica un rango de tiempo personalizado, el gráfico de tendencias se actualiza en consecuencia.

Nombre de la tarjeta	Descripción
	• Los filtros de categoría y acción de DNS resaltan la variable seleccionada en la tarjeta, pero no la eliminan del gráfico.
Distribución de categorías de DNS entre las acciones	Muestra un diagrama de flujo que proporciona una visualización de las distribuciones de acciones tomadas para categorías de DNS de alto riesgo. Una tabla secundaria muestra las acciones realizadas para las categorías de DNS de menor prioridad. • Pase el cursor sobre un flujo específico para abrir una ventana emergente que muestra el número de acciones realizadas del tipo especificado. Cuando especifica un rango de tiempo personalizado, el diagrama de flujo se actualiza automáticamente. • Los filtros de categoría y acción DNS no alteran el contenido de la tarjeta.  • La lista de dominios principales se genera en función de la configuración de filtro que se aplica en la parte superior del panel. Los widgets que afectan la configuración general de la página también determinan qué dominios se muestran. • Pase el cursor sobre una barra para ver las estadísticas de uso. • Haga clic en un dominio para ver los detalles del análisis de DNS.
Dominios	Muestra em número de dominios vistos en su red, dentro de su sector, otras industrias, así como el número total, según la categoría de DNS seleccionada. Le permite comparar el uso de DNS de su organización con otras organizaciones dentro del sector, así como con datos recopilados globalmente, incluida una lista de solicitudes de dominio que se encuentran exclusivamente en su red.

Nombre de la tarjeta	Descripción
	 • Los dominios enumerados en esta tarjeta incluyen todas las categorías de DNS independientemente de la categoría de DNS y los filtros de acción. Sólo el rango de tiempo actualiza el contenido de la tarjeta.
Los 10 dominios principales	Proporciona una lista de los 10 dominios más solicitados de su red junto con la categoría de DNS y la acción realizada. Puede ver más detalles y los logs relevantes de un dominio haciendo clic en el icono apropiado. Seleccione **View All DNS Requests (Ver todas las solicitudes de DNS)** para obtener una lista completa de los dominios a los que se ha accedido.  • Los dominios enumerados en esta tarjeta incluyen todas las categorías de DNS independientemente de la categoría de DNS y los filtros de acción. Sólo el rango de tiempo actualiza el contenido de la tarjeta. • Haga clic en un dominio para ver los detalles del análisis de DNS.
Solucionadores de DNS	Proporcionan dos listas que muestran los dominios maliciosos más resueltos y los dominios menos resueltos en su red.

Nombre de la tarjeta	Descripción
	 • Haga clic en un solucionador de DNS para ver los detalles del análisis de DNS.
Dominios mal configurados (Advanced DNS Security)	Proporciona una lista de dominios que no se pueden resolver asociados con los dominios principales orientados al público especificados por el usuario. Para cada entrada, hay un motivo para la mala configuración y un recuento de resultados de tráfico basado en la IP de origen. 
Dominios secuestrados (Advanced DNS Security)	Proporciona una lista de dominios secuestrados según lo ha determinado Advanced DNS Security. Para cada entrada, hay un motivo para la clasificación y un recuento de resultados de tráfico basado en la IP de origen.

Nombre de la tarjeta	Descripción
	

Ver Panel de DNS Security (Strata Cloud Manager)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

STEP 2 | Seleccione **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **DNS Security** para abrir el panel de DNS Security.

STEP 3 | Desde el panel de control, configure las opciones de filtro utilizando los menús desplegables disponibles.

1. Filtrar por rango de tiempo: seleccione entre **Last hour (Última hora)**, **Last 24 hours (Últimas 24 horas)**, **Last 7 days (Últimos 7 días)** o **Last 30 days (Últimos 30 días)** para mostrar datos para un periodo de tiempo específico.
2. Filtre por categoría de DNS: seleccione entre **Select All (Seleccionar todo)**, **MalwareCommand and Control (Comando y control)**, **Phishing**, **Grayware**, **Exceptions List (Listas de excepciones)**, **Newly Registered (Recientemente registrado)**, **Dynamic DNS (DNS dinámico)**, **Proxy**, **Parked (Estacionado)**, **Benign (Benigno)**, **Ad Track (Seguimiento de anuncios)** para filtrar el conjunto de datos según un tipo de DNS.

   La categoría Lista de excepciones es una lista de dominios explícitamente permitidos según métricas de PAN-DB y Alexa, y mantenida por Palo Alto Networks. Estos dominios de la lista de permitidos son visitados con frecuencia y se sabe que no tienen contenido malicioso.
3. Filtrar por acción DNS: seleccione entre **Allow (Permitir)**, **Block (Bloquear)** y **Sinkhole (Sumidero)** para filtrar según la acción realizada en una consulta DNS según la configuración de la acción de su perfil de DNS Security.

STEP 4 | Opcionalmente, también puede Descargar, Compartir y Programar informes de actividad.

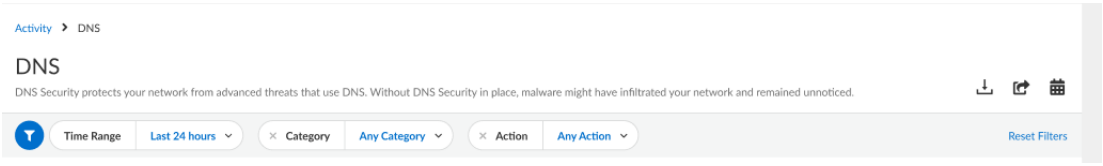
STEP 5 | Puede volver a contextualizar, interactuar y pivotar a partir de los datos proporcionados por las tarjetas del panel. Para obtener una visión general de cada una de las tarjetas del panel de DNS Security, consulte Tarjetas del panel de DNS Security.

Ver Panel de DNS Security (AIOps for NGFW Free)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en la aplicación de AIOps for NGFW Free en el hub.

STEP 2 | Seleccione **Dashboards (Paneles)** > **More Dashboards (Más paneles)** > **DNS Security** para abrir el panel de DNS Security.

STEP 3 | Desde el panel de control, configure las opciones de filtro utilizando los menús desplegables disponibles.



1. Filtrar por rango de tiempo: seleccione entre **Last hour (Última hora)**, **Last 24 hours (Últimas 24 horas)**, **Last 7 days (Últimos 7 días)** o **Last 30 days (Últimos 30 días)** para mostrar datos para un periodo de tiempo específico.
2. Filtrar por categoría de DNS: seleccione entre **C2 (DGA, Tunneling, other C2 [C2 (DGA, túneles, otros C2)]**, **malware**, **Newly Registered Domain (Dominio recientemente registrado)**, **phishing**, **Dynamic DNS (DNS dinámico)**, **Allow List (Lista de permitidos)**, **Benign (Benigno)**, **Grayware**, **Parked (Estacionado)**, **Proxy** y **Any Category (Cualquier categoría)**, para filtrar el conjunto de datos en función de un tipo de DNS.

   La categoría Lista de permitidos es una lista de dominios explícitamente permitidos basados en métricas de PAN-DB y Alexa y mantenida por Palo Alto Networks. Estos dominios de la lista de permitidos son visitados con frecuencia y se sabe que no tienen contenido malicioso.
3. Filtrar por acción DNS: seleccione entre **Allow (Permitir)**, **Block (Bloquear)** y **Sinkhole (Sumidero)** para filtrar según la acción realizada en una consulta DNS según la configuración de la acción de su perfil de DNS Security.

STEP 4 | Opcionalmente, también puede Descargar, Compartir y Programar informes de actividad.

STEP 5 | Puede volver a contextualizar, interactuar y pivotar a partir de los datos proporcionados por las tarjetas del panel. Para obtener una visión general de cada una de las tarjetas del panel de DNS Security, consulte Tarjetas del panel de DNS Security.

Ver logs de DNS Security

¿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) • VM-SERIES • CN-Series	❑ Licencia de Advanced DNS Security (para un mejor soporte de funciones) o Licencia de DNS Security ❑ Licencia de Advanced Threat Prevention o Threat Prevention

Puede explorar, buscar y ver los logs de DNS Security que se generan automáticamente cuando DNS Security se encuentra con un evento cualificado. Normalmente, esto incluye cualquier categoría de dominio que DNS Security analiza a menos que esté configurado específicamente con un nivel de gravedad de logs de ninguno. Las entradas de log proporcionan numerosos detalles sobre el evento, incluido el nivel de amenaza y, si corresponde, la naturaleza de la amenaza.

Los logs de DNS Security están accesibles directamente en el cortafuegos o a través de visores de logs basados en Strata Logging Service (AIOps for NGFW Free, Cloud Management, Strata Logging Service, etc.). Si bien el cortafuegos le permite acceder a entradas de logs de amenazas maliciosas que se generan cuando los usuarios realizan consultas DNS, las solicitudes de DNS benignas no se registran. Los datos de DNS Security también se reenvían al Strata Logging Service a través del reenvío de logs (como logs de amenazas) y la telemetría de DNS Security (como logs de DNS Security), a los que luego se hace referencia mediante varias aplicaciones del visor de logs de actividad. La telemetría de DNS Security opera con una sobrecarga mínima, lo que limita la cantidad de datos enviados al Strata Logging Service; como resultado, solo un subconjunto de consultas DNS se reenvía al Strata Logging Service como entradas de log de DNS Security, independientemente del nivel de gravedad, el tipo de amenaza o la categoría. Los logs de amenazas para las solicitudes de DNS maliciosas que se reenvían a Strata Logging Service mediante el reenvío de logs están disponibles en su totalidad. Como resultado, Palo Alto Networks recomienda ver los logs de solicitudes de DNS maliciosas como logs de amenazas en lugar de logs de DNS Security.

- Strata Cloud Manager
- PAN-OS y Panorama
- AIOps para NGFW gratuita
- Servicio de creación de logs de Strata

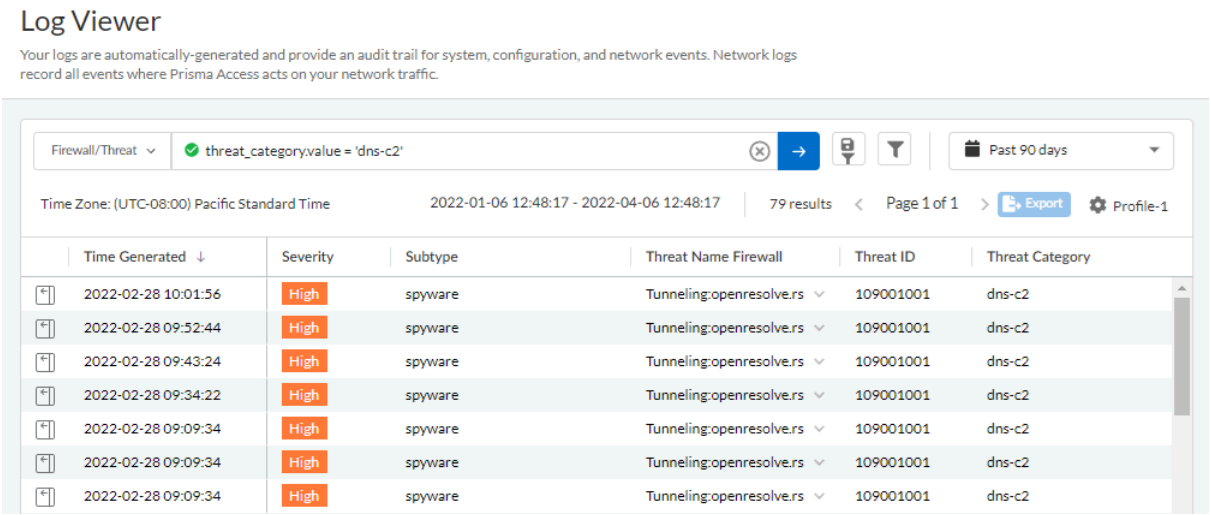
Ver logs de DNS Security(Strata Cloud Manager)

Las consultas DNS benignas analizadas por DNS Security no se muestran en el visor de logs. Inicie sesión en su aplicación Strata Logging Service para acceder a entradas de registros DNS benignas.

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en Strata Cloud Manager en el hub.

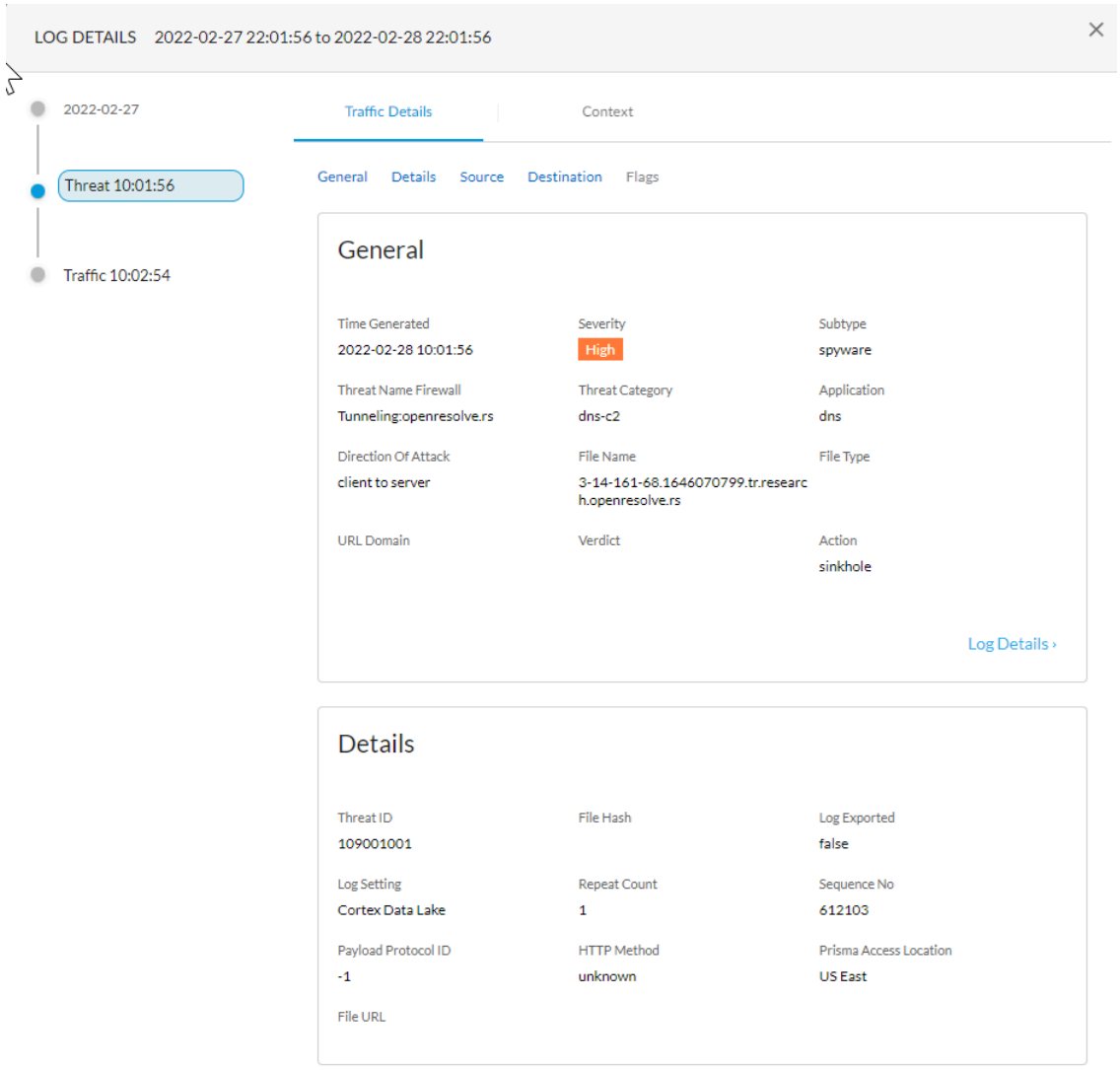
STEP 2 | Busque consultas DNS que se han procesado mediante DNS Security.

1. Seleccione **Incidents and Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
2. Restrinja su búsqueda mediante el filtro de amenazas y envíe una consulta de log basada en la categoría de DNS, por ejemplo, `threat_category.value = 'dns-c2'` para ver los logs que se han determinado que son un dominio C2. Para buscar otros tipos de DNS, reemplace c2 por otra categoría de DNS compatible (ddns, estacionado, malware, etc.). Ajuste los criterios de búsqueda según sea necesario para su búsqueda, incluidos parámetros de consulta adicionales (como el nivel de gravedad y el subtipo) junto con un rango de fechas.



3. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada.

4. La **Category (Categoría)** de amenazas se muestra en el panel **General** de la vista de log detallada. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.



5. Para los dominios almacenados y los dominios de tunelización DNS, incluidos las APT (amenazas persistentes avanzadas) basadas en tunelización, puede ver las diversas herramientas utilizadas en el ataque, así como las campañas de ataque asociadas con el dominio. Esto se refleja en el campo ID/Nombre de amenaza para la entrada de log de un dominio determinado. El ID/Nombre de amenaza para los dominios DNS con atribuciones utiliza el siguiente formato; en este ejemplo, para los dominios de túnel DNS: `Tunelización:<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`, a través del cual el nombre de la herramienta`tool_name` se refiere a las herramientas de tunelización DNS utilizadas para incrustar datos en las consultas y respuestas DNS, pero también el nombre de la campaña de ciberamenaza, en una lista separada por comas. Estas campañas pueden ser incidentes aceptados por la industria y utilizar las mismas convenciones de nomenclatura, o pueden ser identificadas y nombradas por Palo Alto Networks y descritas en los Blogs de investigación de amenazas de Unit 42. Un blog de tal campaña, en este caso,

uno que aprovecha las técnicas de tunelización DNS, se puede encontrar aquí: Aprovechar la Tunelización DNS para el seguimiento y el análisis.

La herramienta asociada y las atribuciones de la campaña pueden tardar algún tiempo después de que la detección inicial se haya completado para ser visibles en los logs, así como en Palo Alto Networks ThreatVault y Test-A-Site. Cuando el componente de atribución finaliza y se ha verificado, las herramientas completas de tunelización DNS y los detalles de la campaña se muestran como se esperaba en los campos ID/Nombre de amenaza y campaña.

Ver logs de DNS Security(NGFW (Managed by PAN-OS or Panorama))

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

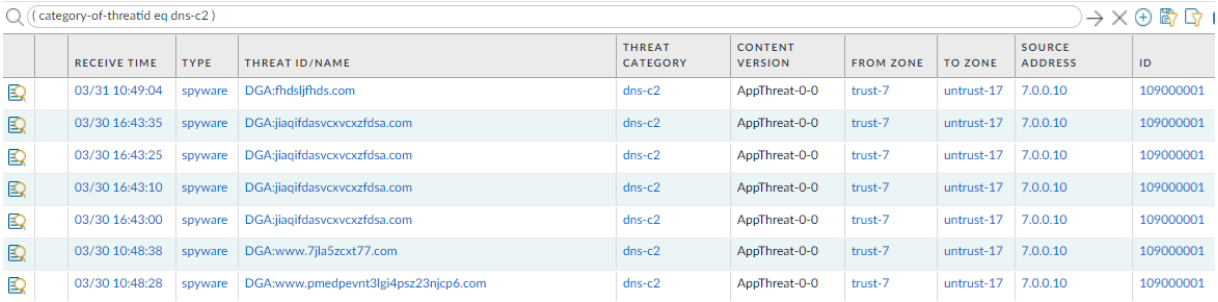
STEP 2 | Busque actividad en el cortafuegos para consultas que se han procesado utilizando DNS Security.

1. Seleccione **Monitor (Supervisar)** > **Logs (Logs)** > **Threat (Amenaza)** y filtre según la categoría de DNS.

   Considere los siguientes ejemplos:

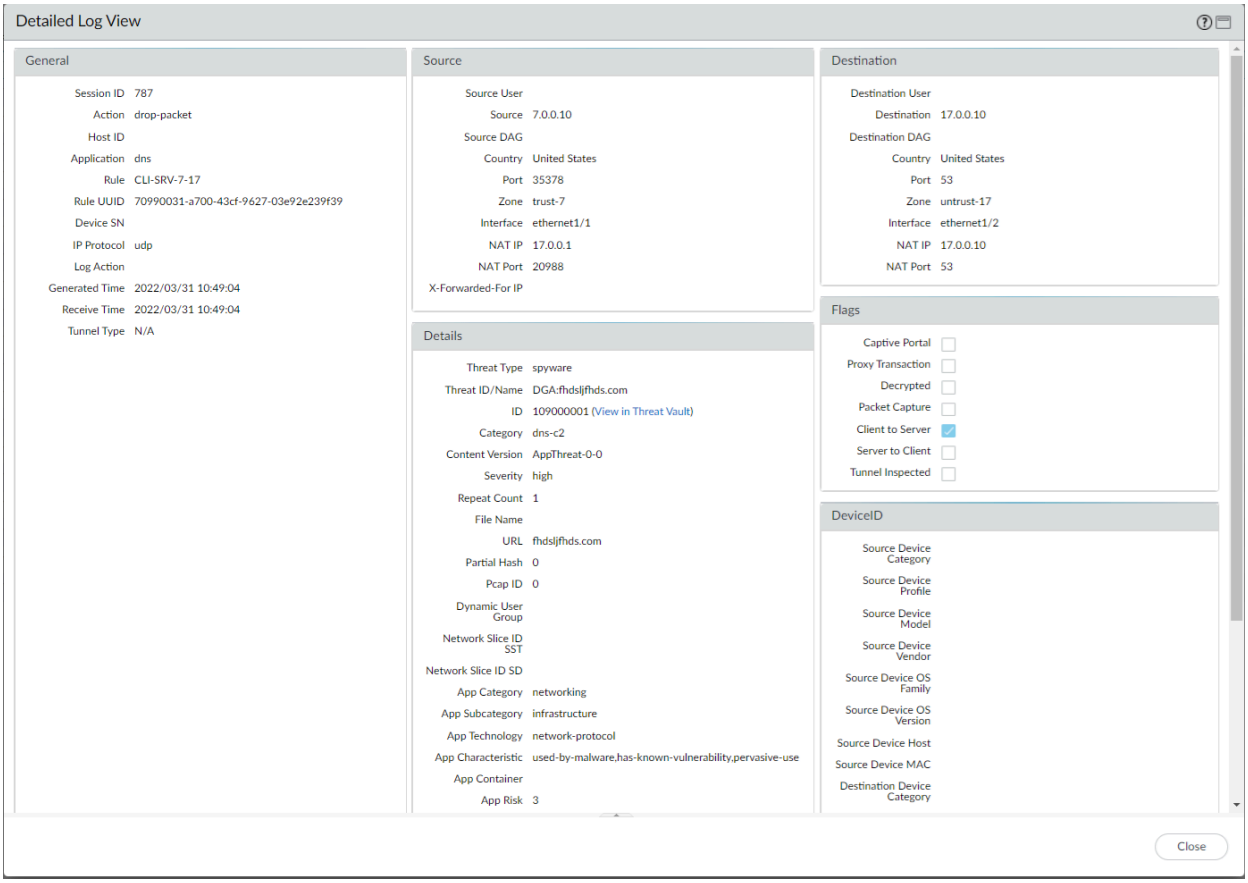
   - `( category-of-threatid eq dns-c2 )` para ver los logs que DNS Security ha considerado que son un dominio C2.
   - `( category-of-threatid eq adns-hijacking )`, por el cual la variable `adns-hijacking` indica consultas DNS que Advanced DNS Security ha clasificado como un intento de secuestro DNS malicioso.

   Para buscar otros tipos de DNS, reemplace c2 por otra categoría de DNS compatible (ddns, estacionado, malware, etc.).



	RECEIVE TIME	TYPE	THREAT ID/NAME	THREAT CATEGORY	CONTENT VERSION	FROM ZONE	TO ZONE	SOURCE ADDRESS	ID
	03/31 10:49:04	spyware	DGA:fhdsljfhds.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:35	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:25	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:10	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:00	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:38	spyware	DGA:www.7jla5zcxt77.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:28	spyware	DGA:www.pmedpevnt3lgi4psz23njcp6.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001

2. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada.
3. La **Category (Categoría)** de amenaza se muestra en el panel **Details (Detalles)** de la vista de log detallada. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.



4. Para los dominios almacenados y los dominios de tunelización DNS, incluidos las APT (amenazas persistentes avanzadas) basadas en tunelización, puede ver las diversas herramientas utilizadas en el ataque, así como las campañas de ataque asociadas con el dominio. Esto se refleja en el campo ID/Nombre de amenaza para la entrada de log de un dominio determinado. El ID/Nombre de amenaza para los dominios DNS con atribuciones utiliza el siguiente formato; en este ejemplo, para los dominios de túnel DNS: `Tunelización:<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`, a través del cual el nombre de la herramienta`tool_name` se refiere a las herramientas de tunelización DNS utilizadas para incrustar datos en las consultas y respuestas DNS, pero también el nombre de la campaña de ciberamenaza, en una lista separada por comas. Estas campañas pueden ser incidentes aceptados por la industria y utilizar las mismas convenciones de nomenclatura, o pueden ser identificadas y nombradas por Palo Alto Networks y descritas en los Blogs de investigación de amenazas de Unit 42. Un blog de tal campaña, en este caso, uno que aprovecha las técnicas de tunelización DNS, se puede encontrar aquí: Aprovechar la Tunelización DNS para el seguimiento y el análisis. Alternativamente, también puede ver

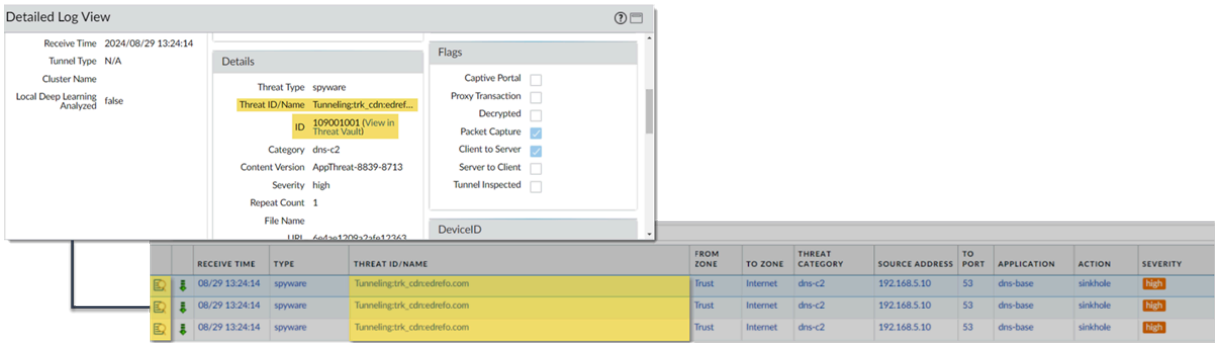
la información de atribución desde ThreatVault y URL Filtering Test A Site de Palo Alto Networks.

La herramienta asociada y las atribuciones de la campaña pueden tardar algún tiempo después de que la detección inicial se haya completado para ser visibles en los logs, así como en Palo Alto Networks ThreatVault y Test-A-Site. Cuando el componente de atribución finaliza y se ha verificado, las herramientas completas de tunelización DNS y los detalles de la campaña se muestran como se esperaba en los campos ID/Nombre de amenaza y campaña.

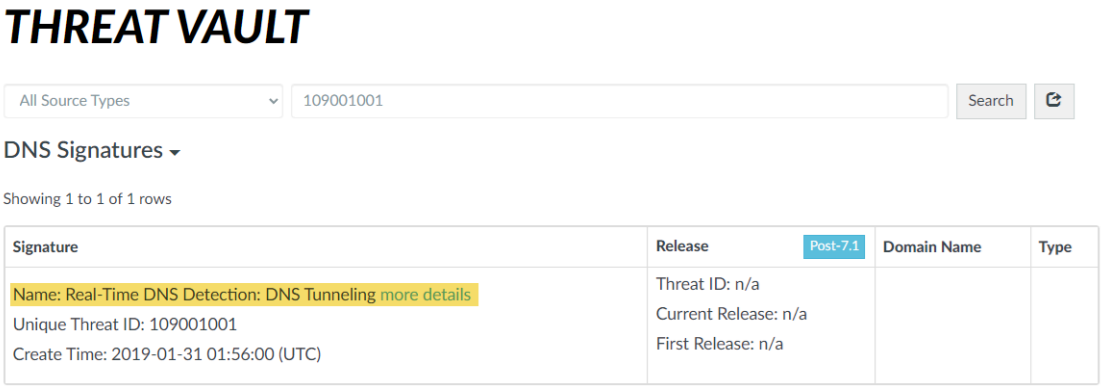
Considere los siguientes ejemplos:

- **Atribución de ATP de dominio de tunelización DNS**

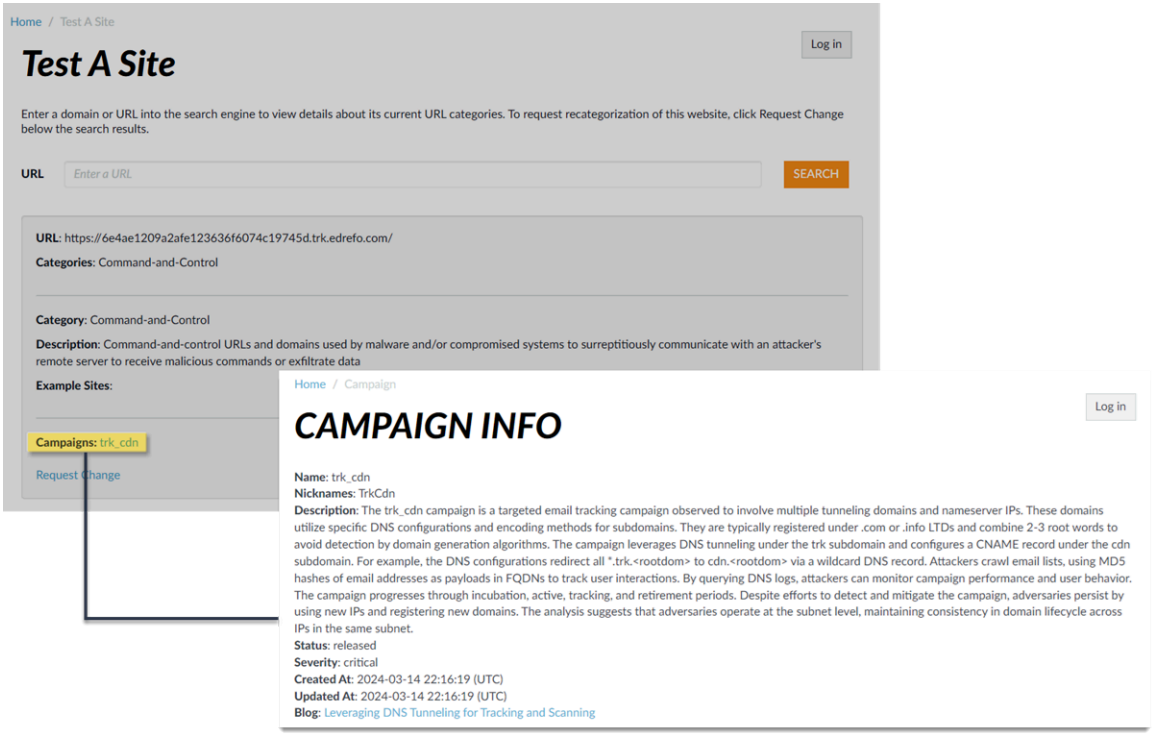
  1. PAN-OS



  2. ThreatVault

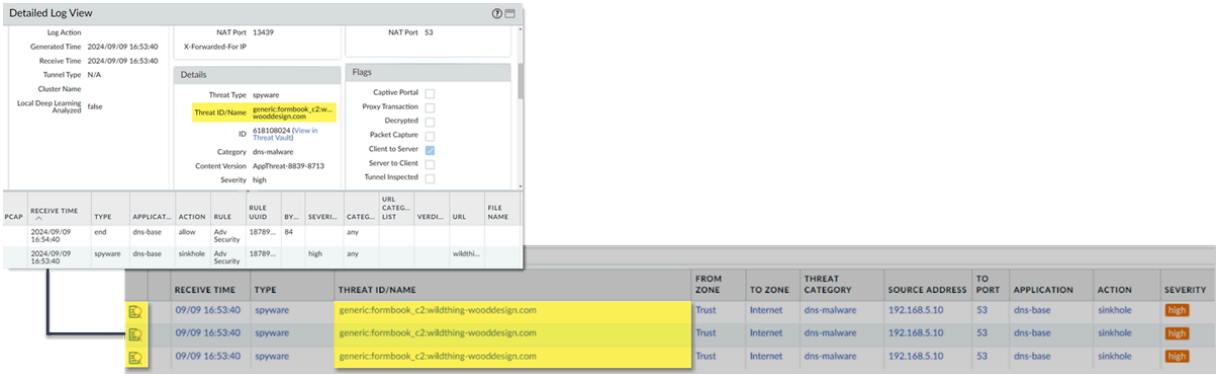


  3. URL Filtering Test-A-Site

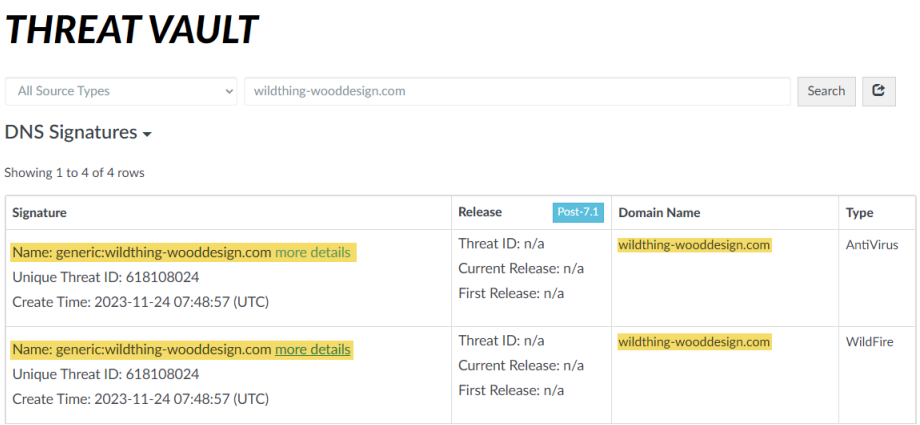


- **Atribución de APT de dominio almacenado**

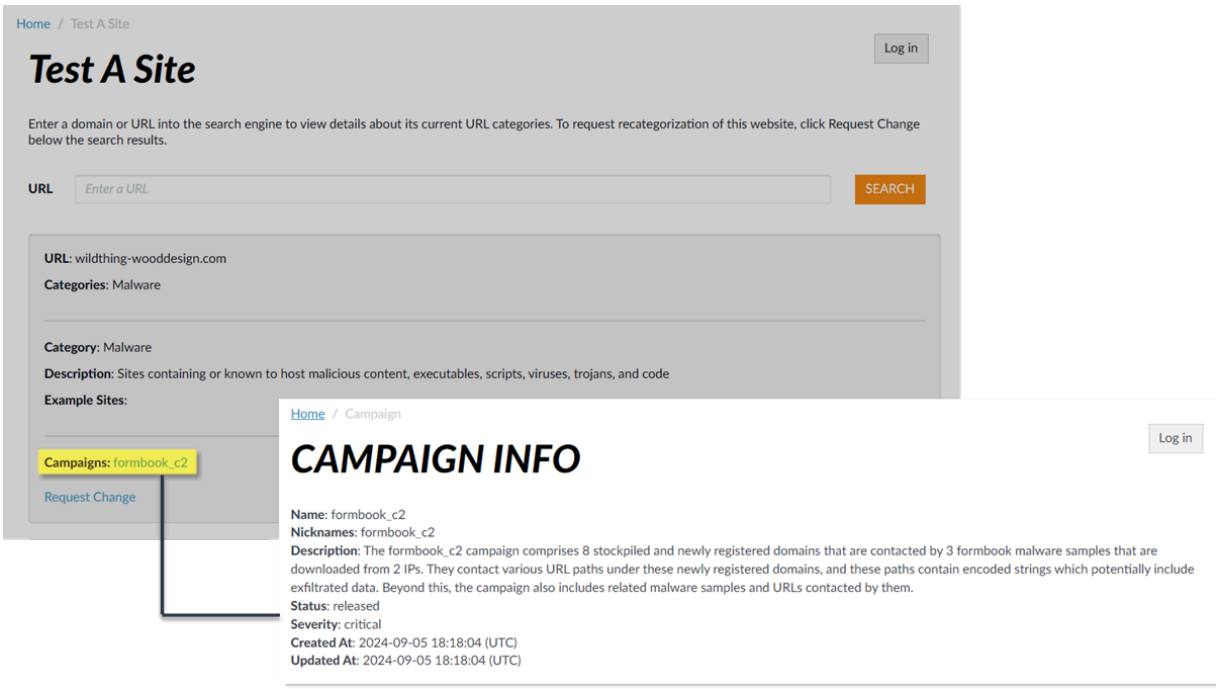
  1. PAN-OS



  2. ThreatVault



3. URL Filtering Test-A-Site



Ver logs de DNS Security(AIOps for NGFW Free)

Las consultas DNS benignas analizadas por DNS Security no se muestran en el visor de logs de AIOps for NGFW Free. Inicie sesión en su aplicación Strata Logging Service para acceder a entradas de registros DNS benignas.

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en la aplicación de AIOps for NGFW Free en el hub.

STEP 2 | Busque consultas DNS que se han procesado utilizando DNS Security en AIOps for NGFW Free.

1. Seleccione **Incidents and Alerts (Incidentes y alertas)** > **Log Viewer (Visor de logs)**.
2. Restrinja su búsqueda mediante el filtro de amenazas y envíe una consulta de log basada en la categoría de DNS, por ejemplo, `threat_category.value = 'dns-c2'` para ver los logs que se han determinado que son un dominio C2. Para buscar otros tipos de DNS, reemplace c2 por otra categoría de DNS compatible (ddns, estacionado, malware, etc.). Ajuste los criterios de búsqueda según sea necesario para su búsqueda, incluidos parámetros de consulta adicionales (como el nivel de gravedad y el subtipo) junto con un rango de fechas.
3. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada.
4. La **Category (Categoría)** de amenaza se muestra en el panel **Details (Detalles)** de la vista de log detallada. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.

Ver logs de DNS Security(Strata Logging Service)

STEP 1 | Utilice las credenciales asociadas con su cuenta de asistencia técnica de Palo Alto Networks e inicie sesión en la aplicación de Strata Logging Service en el hub.

STEP 2 | Asignar almacenamiento según el tipo de log. Si no se ha asignado espacio de almacenamiento para los logs de DNS Security en Strata Logging Service, las entradas de creación de logs no serán visibles a través de Strata Logging Service.

STEP 3 | Busque consultas DNS que se han procesado utilizando DNS Security en Strata Logging Service.

1. Seleccione **Explore (Explorar)** para abrir el Visor de logs de Strata Logging Service.
2. Restrinja su búsqueda mediante el filtro de amenazas y envíe una consulta de log basada en la categoría de DNS, por ejemplo, `threat_category.value = 'dns-c2'` para ver los logs que se han determinado que son un dominio C2. Para buscar otros tipos de DNS, reemplace c2 por otra categoría de DNS compatible (ddns, estacionado, malware, etc.). Ajuste los criterios de búsqueda según sea necesario para su búsqueda, incluidos parámetros de consulta adicionales (como el nivel de gravedad y el subtipo) junto con un rango de fechas.
3. Seleccione una entrada de log para ver los detalles de una amenaza DNS detectada.
4. La **Category (Categoría)** de amenaza se muestra en el panel **Details (Detalles)** de la vista de log detallada. Otros detalles relevantes sobre la amenaza se muestran en sus correspondientes ventanas.

