Solución de problemas de flujo de trabajo de Secure Access Decryption and Intrusion Prevention System (IPS)

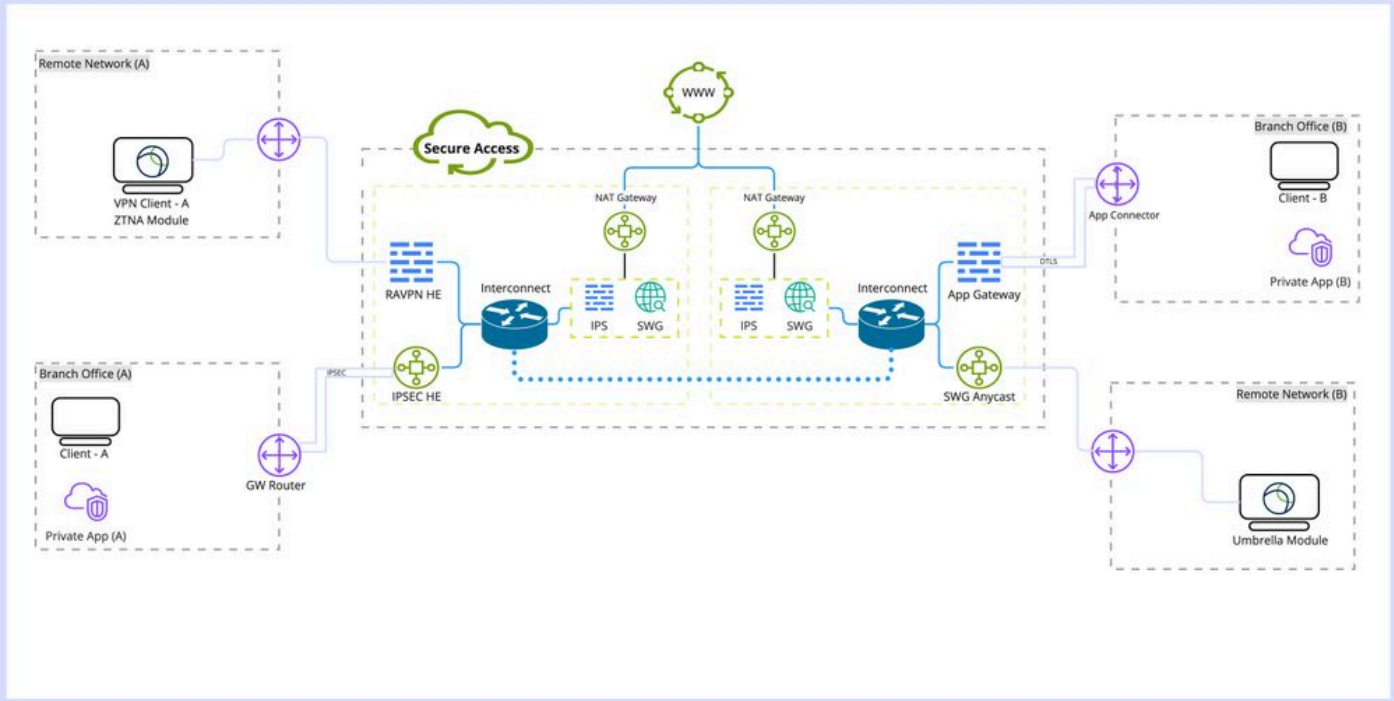
Contenido

Introducción

En este documento se describe el flujo de trabajo de IPS y descifrado de acceso seguro y se resaltan las propiedades de configuración importantes.

Arquitectura de acceso seguro

Esta arquitectura de acceso seguro destaca los diferentes servicios que proporciona Secure Access y los diferentes métodos de conexión que se pueden establecer para proteger la red.



Arquitectura de acceso seguro

Detalles de la arquitectura:

Términos que debe conocer:

RAVPN HE: terminal de red privada virtual de acceso remoto

IPSEC HE: Extremo final de seguridad de protocolo de Internet de túnel remoto (IPSEC)

Módulo ZTNA: Módulo de acceso a la red de confianza cero

SWG: Gateway web seguro

IPS: Sistema de prevención de intrusiones

Gateway NAT: Gateway de traducción de direcciones de red

SWG AnyCast: Secure Web Gateway Anycast punto de entrada

Tipos de implementación:

1. VPN de acceso remoto

2. Túnel de acceso remoto

3. Módulo Umbrella Roaming

4. Conector de la aplicación/gateway de la aplicación

5. Módulo de confianza cero (ZTNA)

Descripción general de características

Secure Access ofrece la posibilidad de utilizar tanto el descifrado web como el sistema de prevención de intrusiones (IPS) para mejorar la detección y la categorización de las aplicaciones, así como para proporcionar más detalles sobre el tráfico, incluidas las rutas URL, los nombres de archivo y sus categorías de aplicación. Además, ayuda a evitar ataques de día cero y malware.

Descifrado: en este artículo, el descifrado se refiere al descifrado del tráfico del protocolo de transferencia de hipertexto (HTTPS) a través del módulo de gateway web seguro (SWG) y también al descifrado del tráfico para la inspección de IPS.

IPS: sistema de detección y prevención de intrusiones a nivel de firewall que requiere descifrado para el tráfico con el fin de realizar la funcionalidad completa.

El descifrado es necesario para varias funciones de acceso seguro, como la prevención de la pérdida de datos (DLP) y el aislamiento del explorador remoto (RBI), la inspección de archivos, el análisis de archivos y el bloqueo de tipos de archivos.

Configuración relacionada con IPS y descifrado en Secure Access

Esta es una descripción general rápida de los parámetros de descifrado e IPS disponibles en Secure Access.

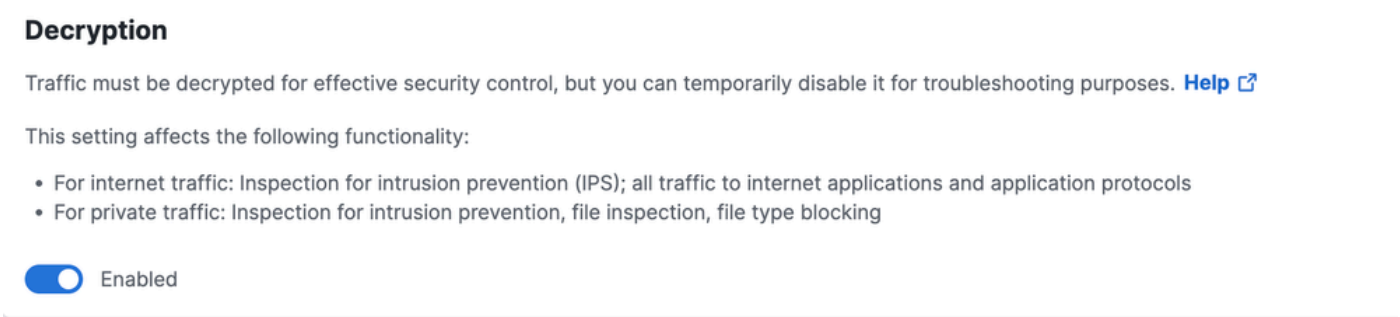
Descifrado para IPS

Esta es una configuración global para IPS que se utiliza para desactivar o activar el motor IPS para todas las políticas.

Propiedades:

- Esta opción no afecta al descifrado de gateway web seguro (descifrado web)
- La desactivación y activación del IPS por política está disponible con funcionalidad limitada para inspeccionar solamente la fase inicial del protocolo de enlace sin inspeccionar el cuerpo de la solicitud.

Configuración: Panel -> Seguro -> Política de acceso -> Valores predeterminados de regla y configuración global -> Configuración global -> Descifrado para IPS



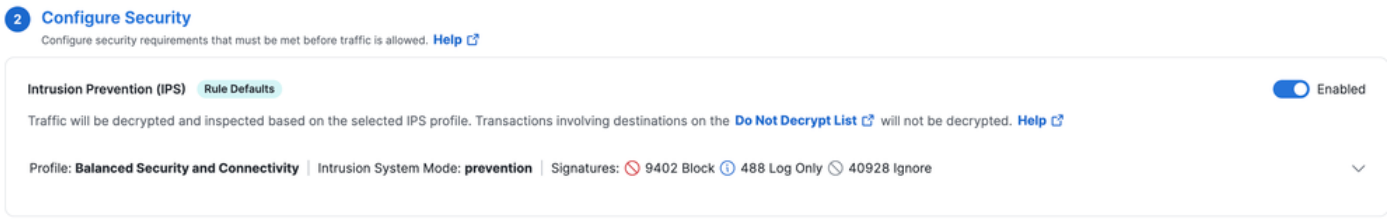
Configuración de IPS por política

Esta opción permite desactivar y activar IPS por bases de políticas.

Propiedades:

- Esta opción controla si IPS está activado o desactivado por directiva.
- Esta opción depende de la opción Descifrar para IPS; si la opción Descifrar para IPS global está deshabilitada, el comportamiento sólo inspeccionará la fase inicial del protocolo de enlace sin inspeccionar el cuerpo de la solicitud.
- Esta opción no afecta al SWG (descifrado web)

Configuración: Panel -> Segura -> Política de acceso ->Editar política -> Configurar seguridad -> Prevención de intrusiones (IPS)



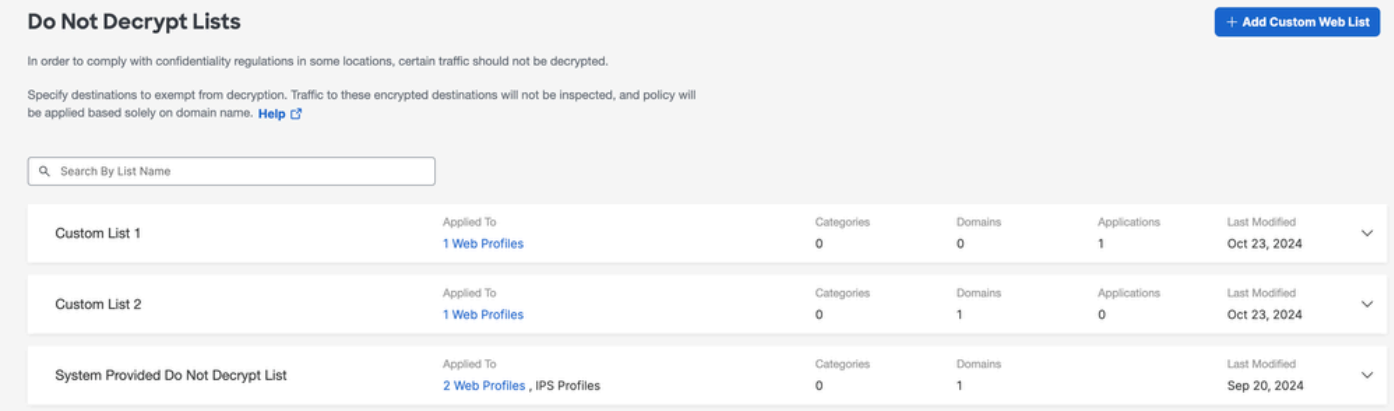
No descifrar listas

Conjunto de listas de destino que se pueden vincular al perfil de seguridad para evitar que los dominios o las direcciones IP se descifren.

Propiedades:

- Permitir que los dominios personalizados se omitan mediante descifrado web
- Esta lista sólo afecta al descifrado web, no a IPS, con la excepción de la lista No descifrar proporcionada por el sistema
- Contiene una (lista No descifrar proporcionada por el sistema) que omite el IPS y el descifrado web
- Esta opción debe combinarse con los perfiles de seguridad que se adjuntarán a la política
- Esta lista solo se puede utilizar si el descifrado está habilitado en el perfil de seguridad

Configuración: Panel -> Segura -> No Descifrar Listas



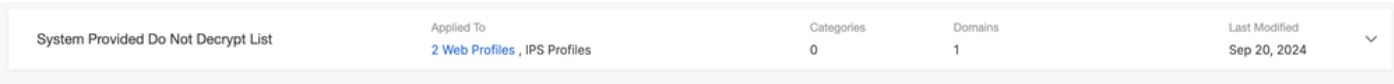
Lista No descifrar proporcionada por el sistema

Parte de las listas No descifrar, con la función adicional de aplicar tanto en el descifrado como en IPS en Secure Access.

Propiedades:

- Esta es la única lista personalizada de No descifrar que afecta tanto al descifrado IPS como al descifrado web
- No existe ninguna opción para personalizar esta lista por directiva.

Configuración: Panel -> Segura -> No Descifrar Listas -> Lista No Descifrar Proporcionada Por El Sistema



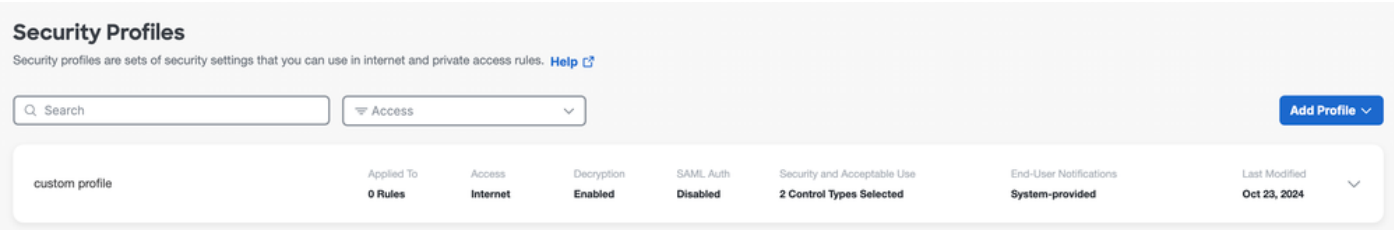
Configuración del perfil de seguridad

En Configuración del perfil de seguridad, puede seleccionar Habilitar o Inhabilitar el descifrado web que se puede asociar posteriormente a una directiva de Internet. Si el descifrado está activado, tiene la opción de seleccionar una de las listas No descifrar configuradas.

Propiedades:

- Controla varias funciones de seguridad, incluidas las listas de descifrado de Web y de no descifrado
- La adición de la lista No descifrar proporcionada por el sistema al perfil de seguridad afecta tanto al descifrado Web como al descifrado IPS

Configuración: Panel -> Segura -> Perfiles de seguridad



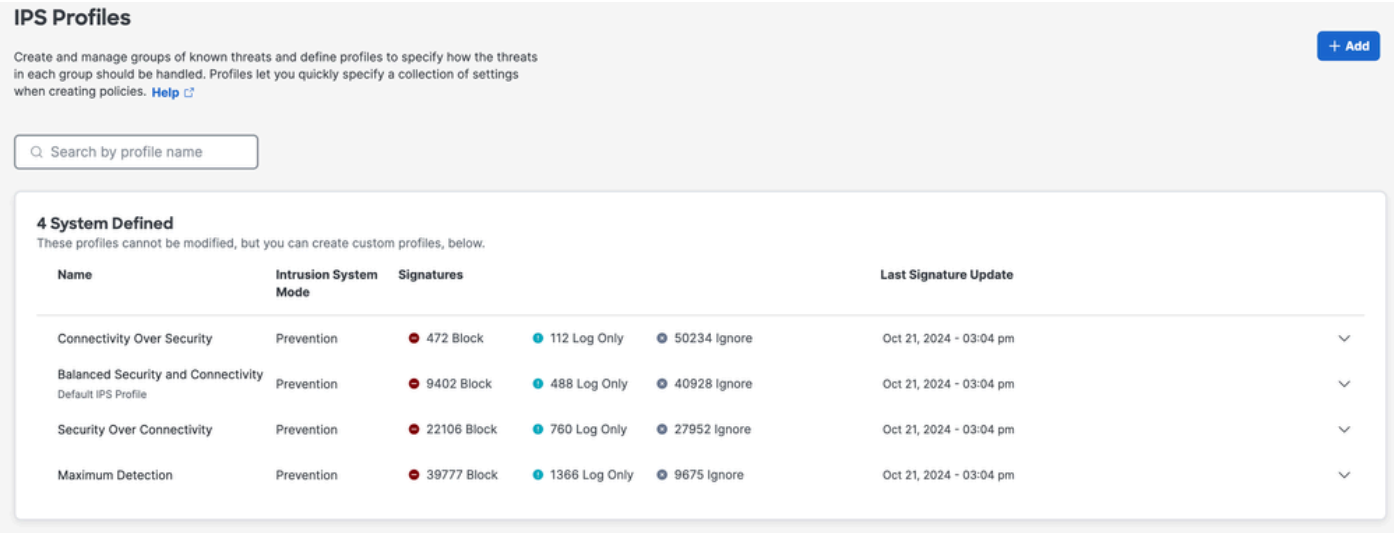
Perfiles IPS

La configuración de los perfiles IPS incluye cuatro parámetros de seguridad predefinidos principales para el perfil IPS. Que se puede seleccionar según la configuración de la política. Tiene la opción de crear su propio perfil IPS personalizado para obtener una configuración más estricta o flexible.

Propiedades:

- Contiene cuatro perfiles de niveles de seguridad predefinidos para IPS
- Se puede crear un perfil IPS personalizado

Configuración: Panel -> Segura -> Perfiles IPS

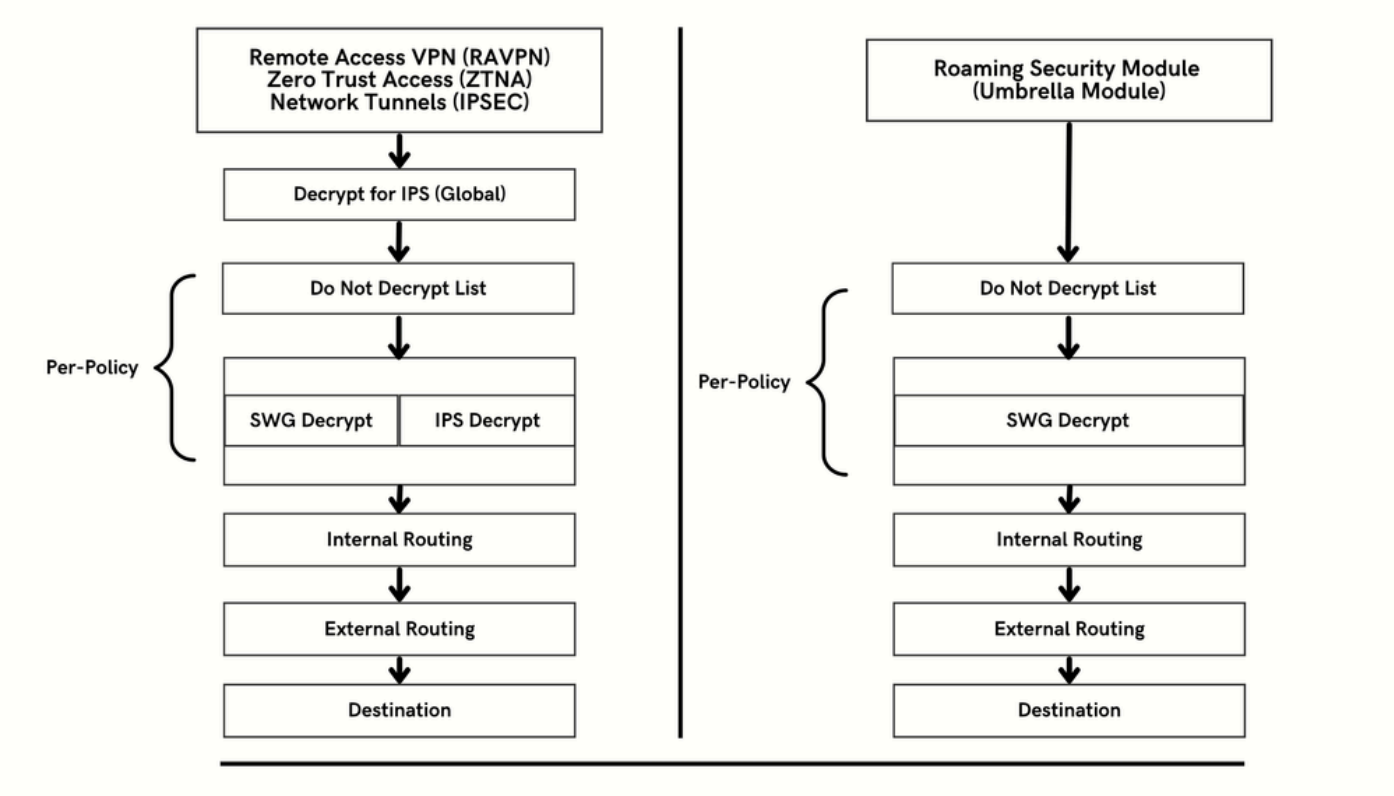


Flujo de tráfico HTTPS en Secure Access

Secure Access tiene diferentes rutas de tráfico basadas en el método de conexión.

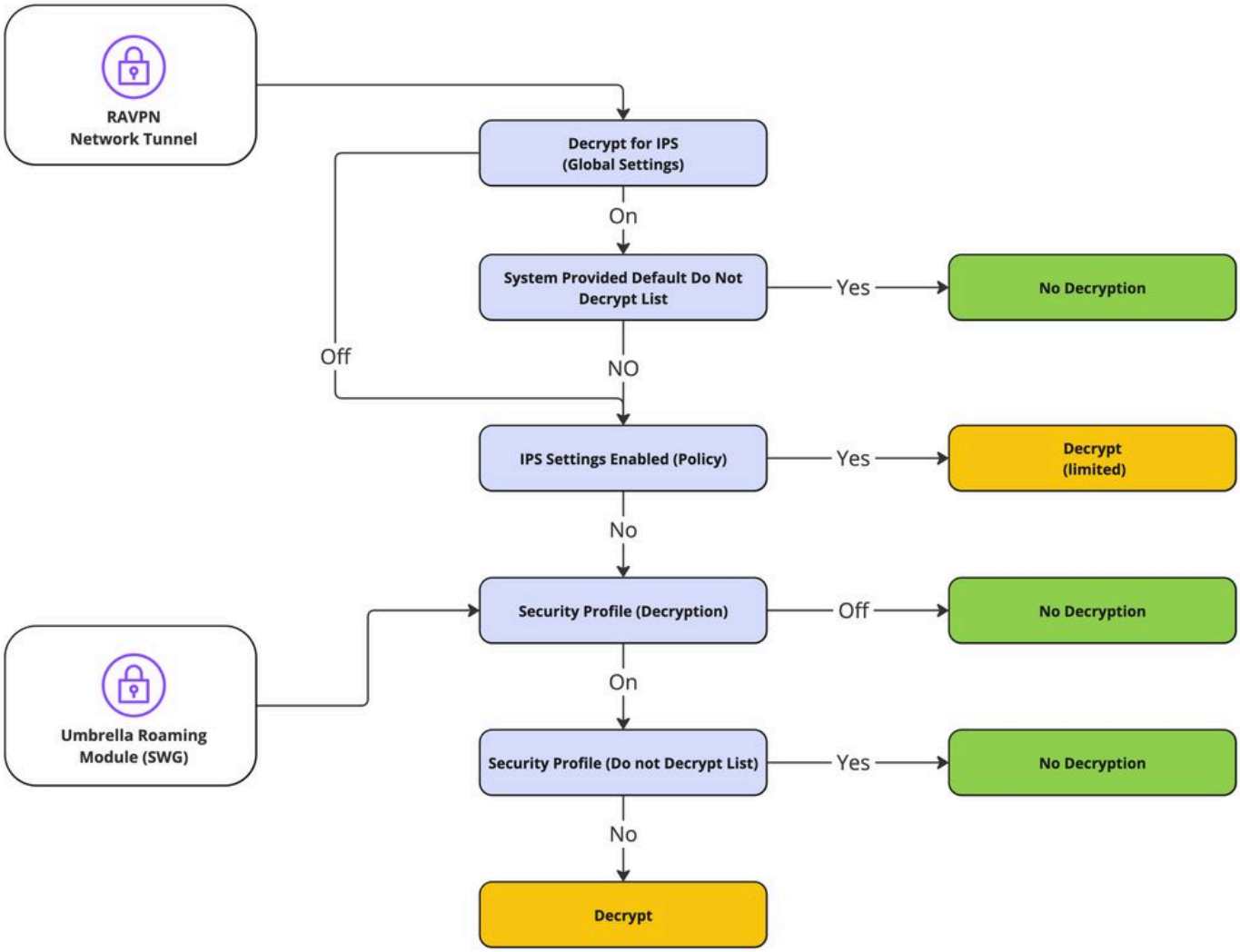
La VPN de acceso remoto (RAVPN) y el acceso de confianza cero (ZTNA) comparten los mismos componentes.

El módulo de seguridad de roaming (módulo Umbrella) tiene una ruta de tráfico diferente.



Cuándo esperar que el tráfico sea descifrado

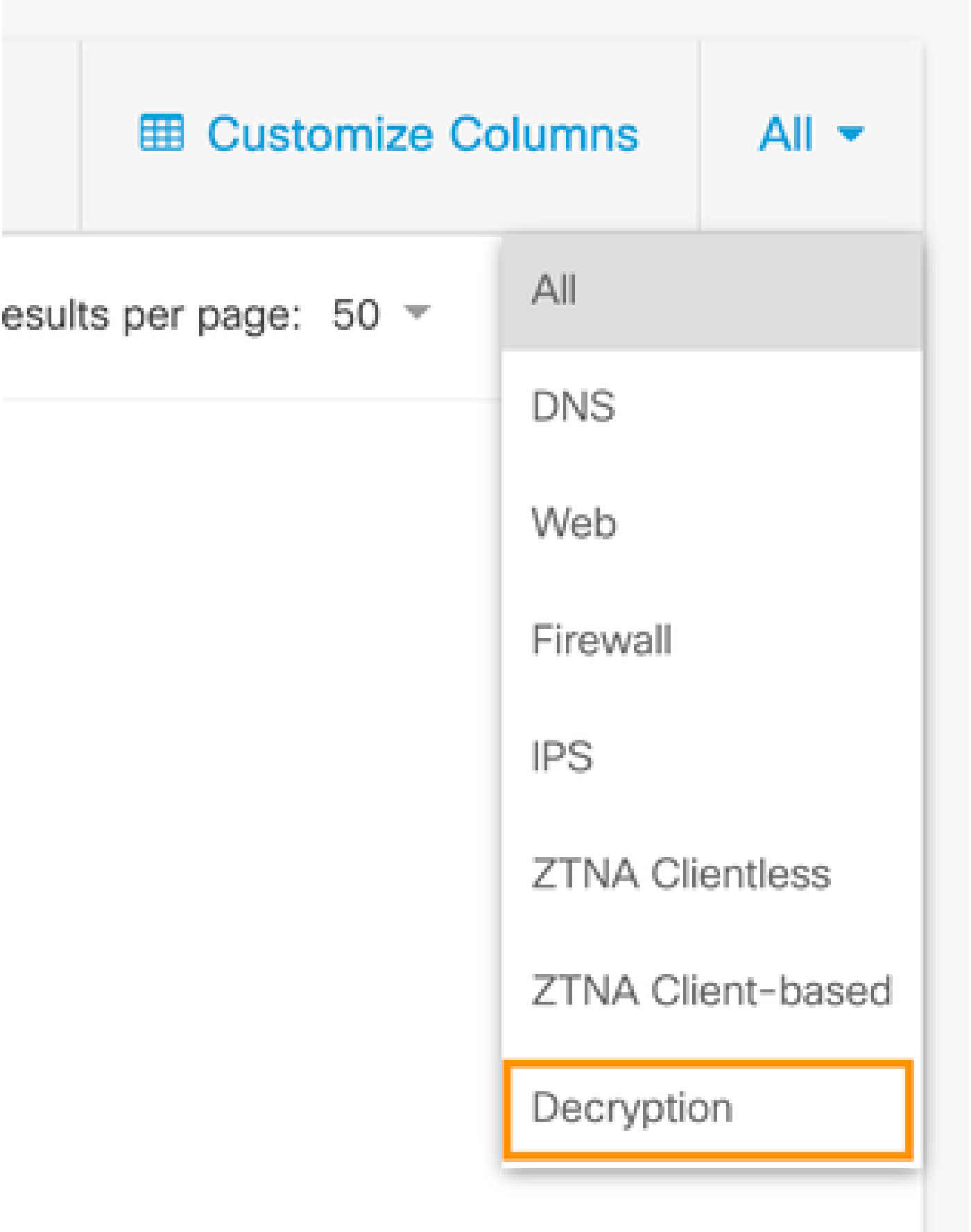
Esta sección explica en detalle la cadena de acciones y sus principales resultados de descifrado o sin descifrado.

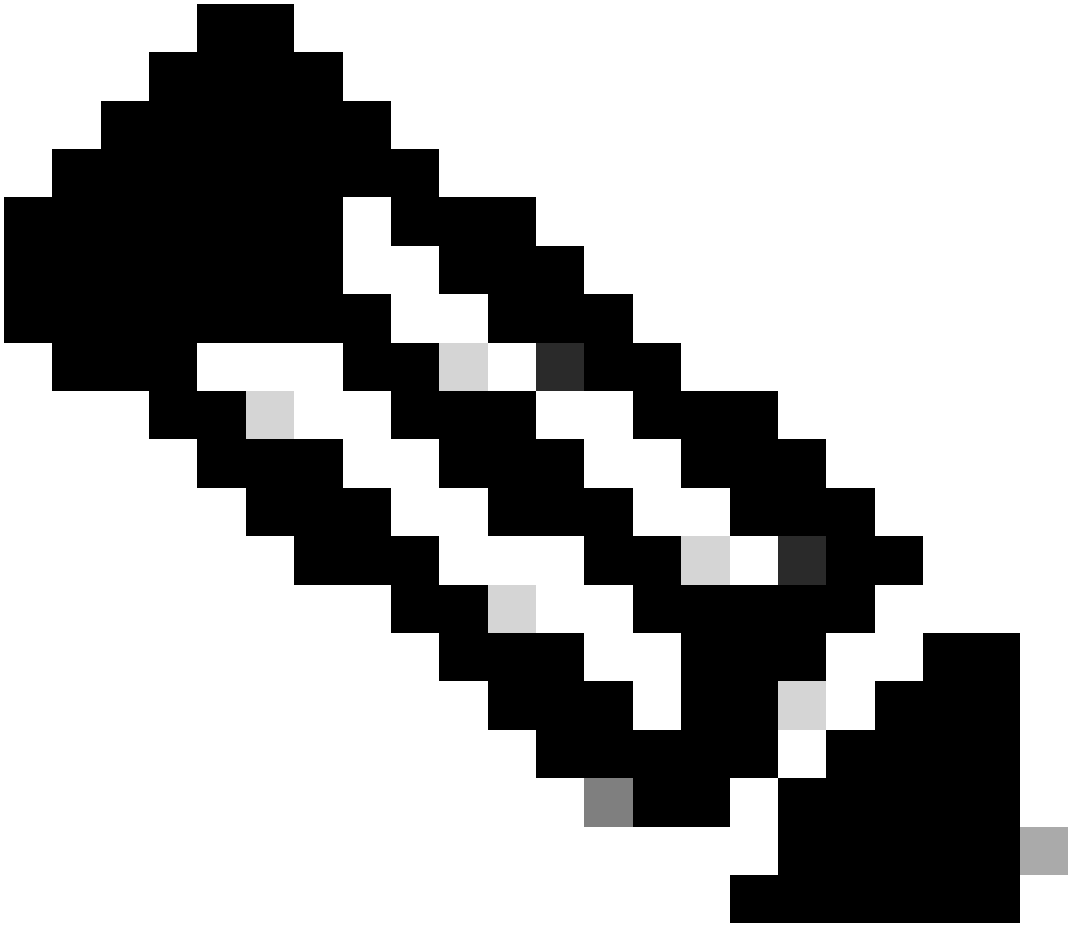


Flujo de descifrado

Registro e informes relacionados con IPS y descifrado

Secure Access incluye una nueva sección de informes (Descifrado) a la que se puede acceder a través del Panel -> Supervisar -> Búsqueda de actividad -> Cambiar al descifrado.

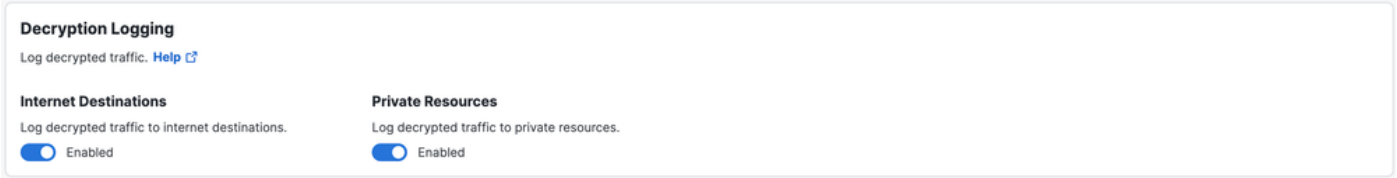

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



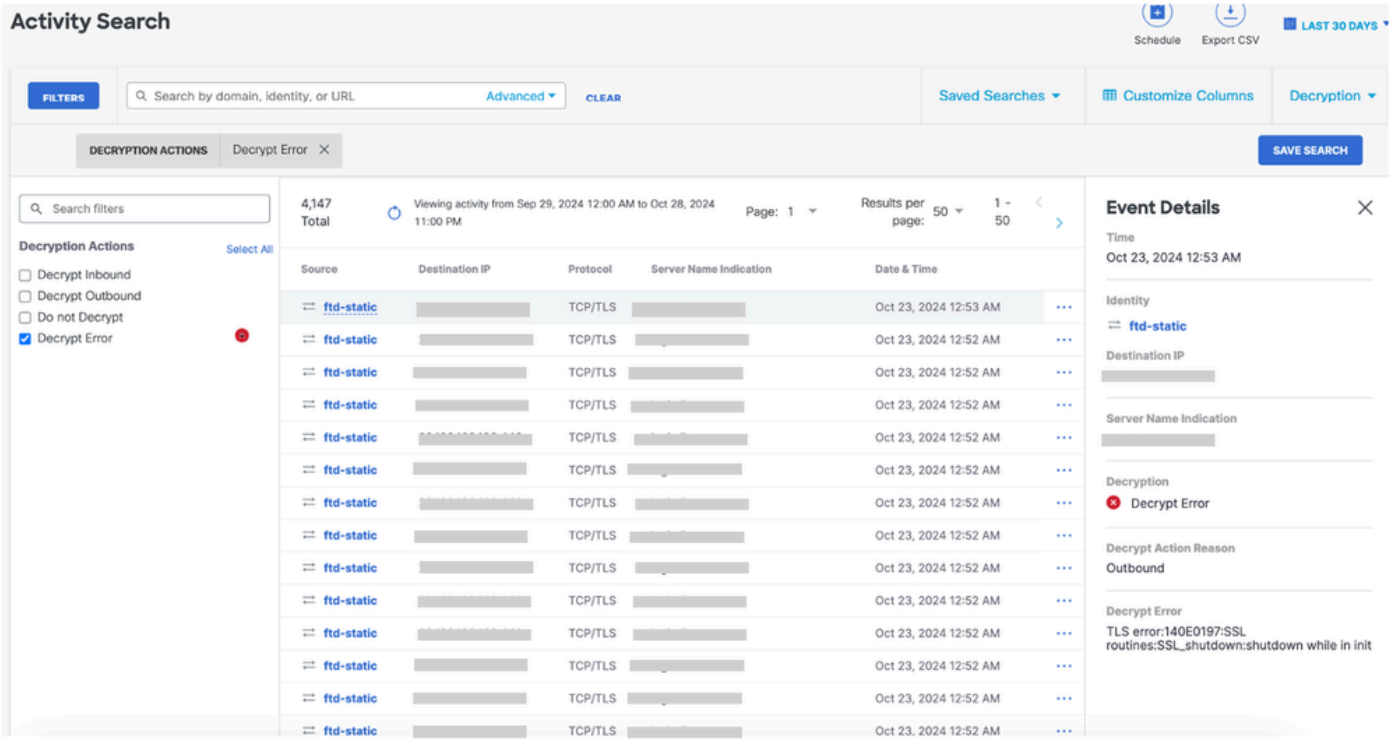
Nota: Para activar los registros de descifrado, esta configuración se puede activar en la configuración global:

Panel -> Seguro -> Directiva de acceso -> Valores predeterminados de regla y configuración global -> Configuración global -> Registro de descifrado.

Configuración de registro de descifrado:



Ejemplo de error de descifrado:



Información Relacionada

- Guía del usuario de Secure Access
- Soporte técnico y descargas: Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).