Configuración de políticas SWG para Umbrella

Contenido

Introducción

Este documento describe cómo configurar políticas web para su uso con Umbrella.

Antecedentes

Bienvenido a Umbrella Secure Web Gateway (SWG). Después de la implementación, el paso más importante es definir una política web para garantizar que el comportamiento básico recibido es el esperado. Hoy en día, este flujo de políticas refleja exactamente las políticas de capa DNS.

Políticas web generales

Las políticas Web de Umbrella funcionan con un algoritmo de aplicación de coincidencia superior. Es decir, se aplica la primera directiva que coincide con el conjunto de identidades actual y se omiten todas las coincidencias de directivas posteriores. Esta es la base de todas las políticas de Umbrella y puede diferir de cualquier expectativa preexistente sobre políticas web basadas en proxy.

Funciones de políticas tal y como se muestran en este diagrama de flujo. La primera coincidencia de política con cualquier identidad incluida en la consulta se aplica sin considerar ninguna otra política.

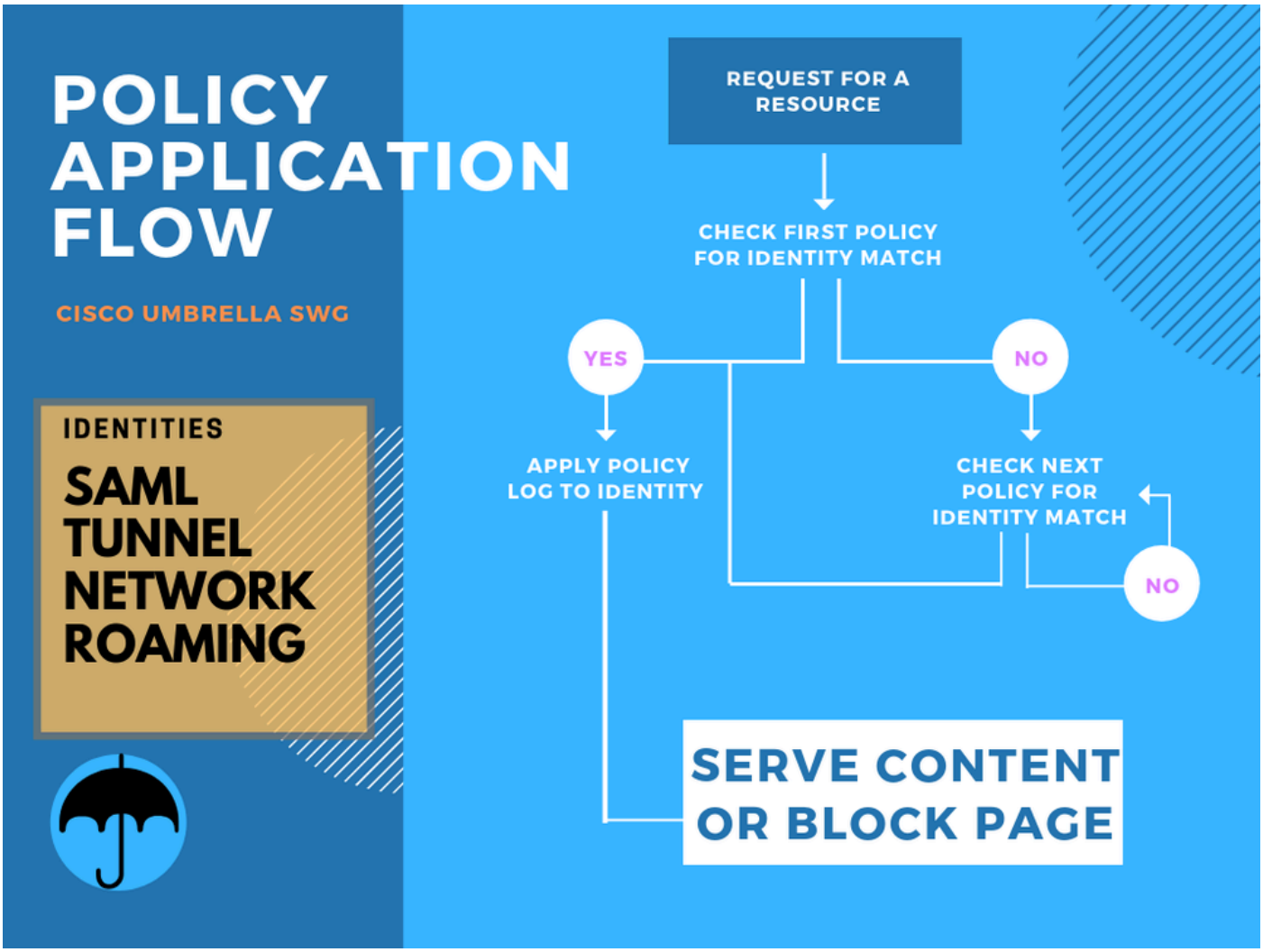


Diagrama de flujo-SWG.png

Dado que este flujo es nuevo para aquellos que no provienen de las políticas de Umbrella DNS, aquí hay un ejemplo de un conjunto de políticas donde varias políticas se aplican al mismo usuario o grupo. Observe cómo sólo se utiliza la primera política que se aplica a Phil (o al grupo de usuarios de Phil) y se ignoran todas las coincidencias restantes. Las coincidencias adicionales no se agregan en la política de Umbrella, simplemente se ignoran.

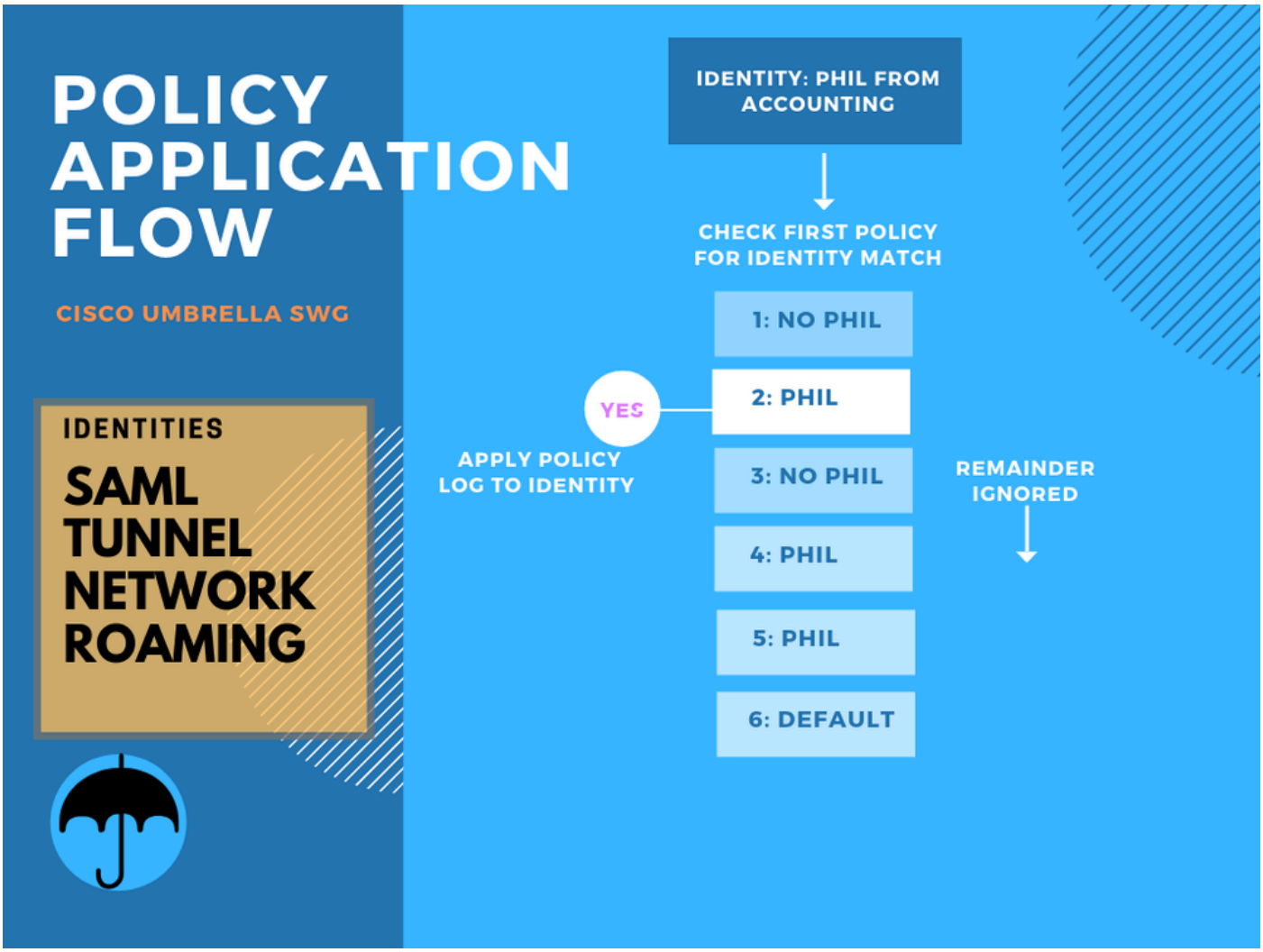


Diagrama de flujo-flow.png

Como resultado, no están disponibles con la política de Umbrella SWG:

- Políticas anidadas
- Permitir y bloquear exclusiones para una aplicación o un sitio web que transciendan cualquier política
    - Ejemplo: Las exclusiones de políticas para Phil son permitir Facebook, permitir Instagram y permitir la exclusión de Dropbox, pero Phillis solo está en permitir Facebook y permitir Instagram.
        - En la política general, se trataría de dos políticas únicas.
            - Permitir Facebook, Instagram, Dropbox aplicar a Phil
            - Permitir Facebook, Instagram aplicar a Phillis
        - Cada combinación de aplicaciones individuales permitidas o bloqueadas debe tener una nueva política creada con los usuarios aplicables agregados a la política.

Además, cualquier tráfico que no sea HTTP/S recibe la política de capa DNS para este tipo de tráfico.

Notas importantes sobre Cloud Delivered Firewall y SWG

El CDFW de Umbrella envía cualquier tráfico HTTP/S permitido a través del SWG de Umbrella y, por lo tanto, también aplica la política. Una vez que se define una política, el flujo de aplicación de la política funciona igual que el flujo SWG.

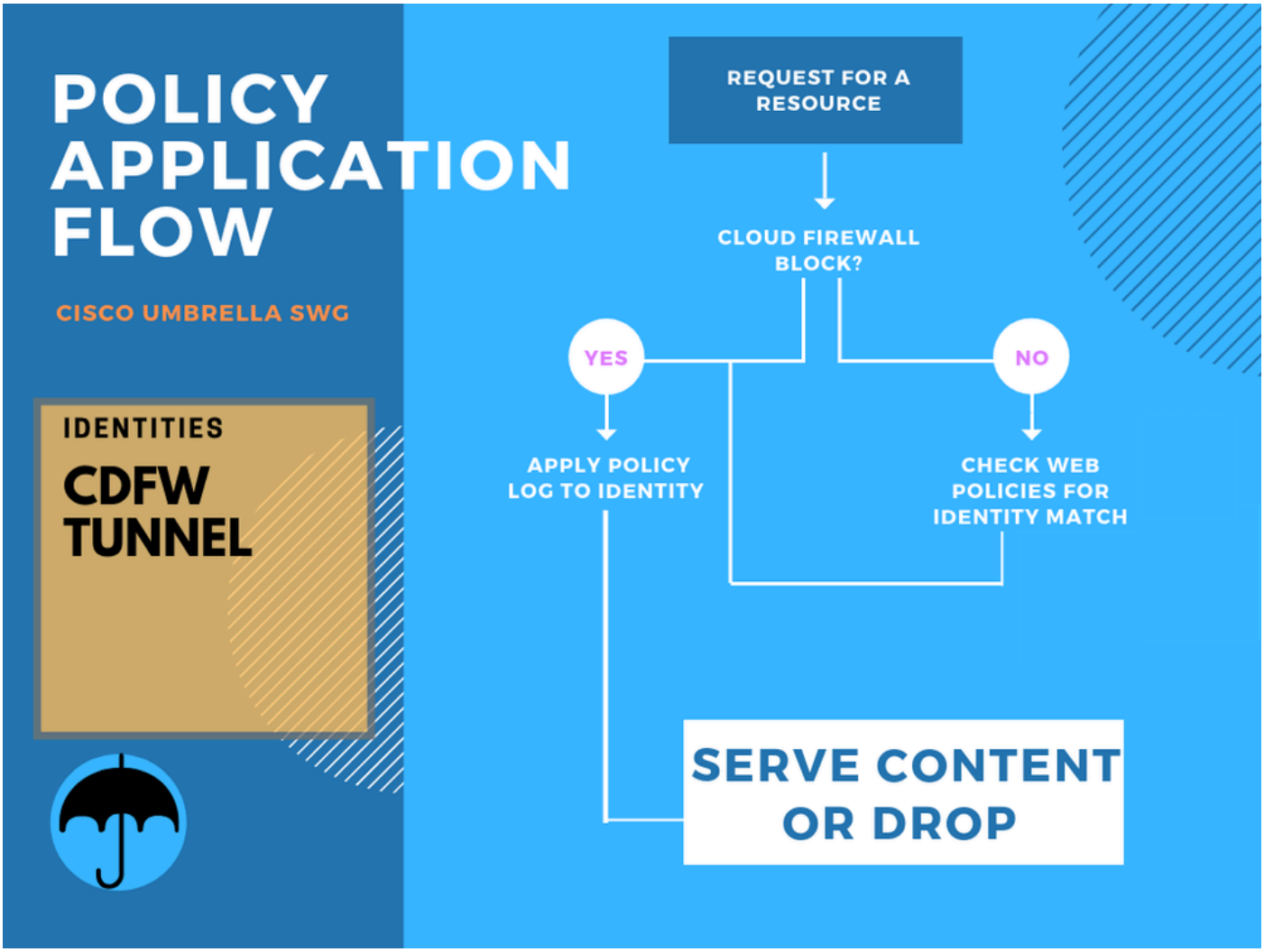


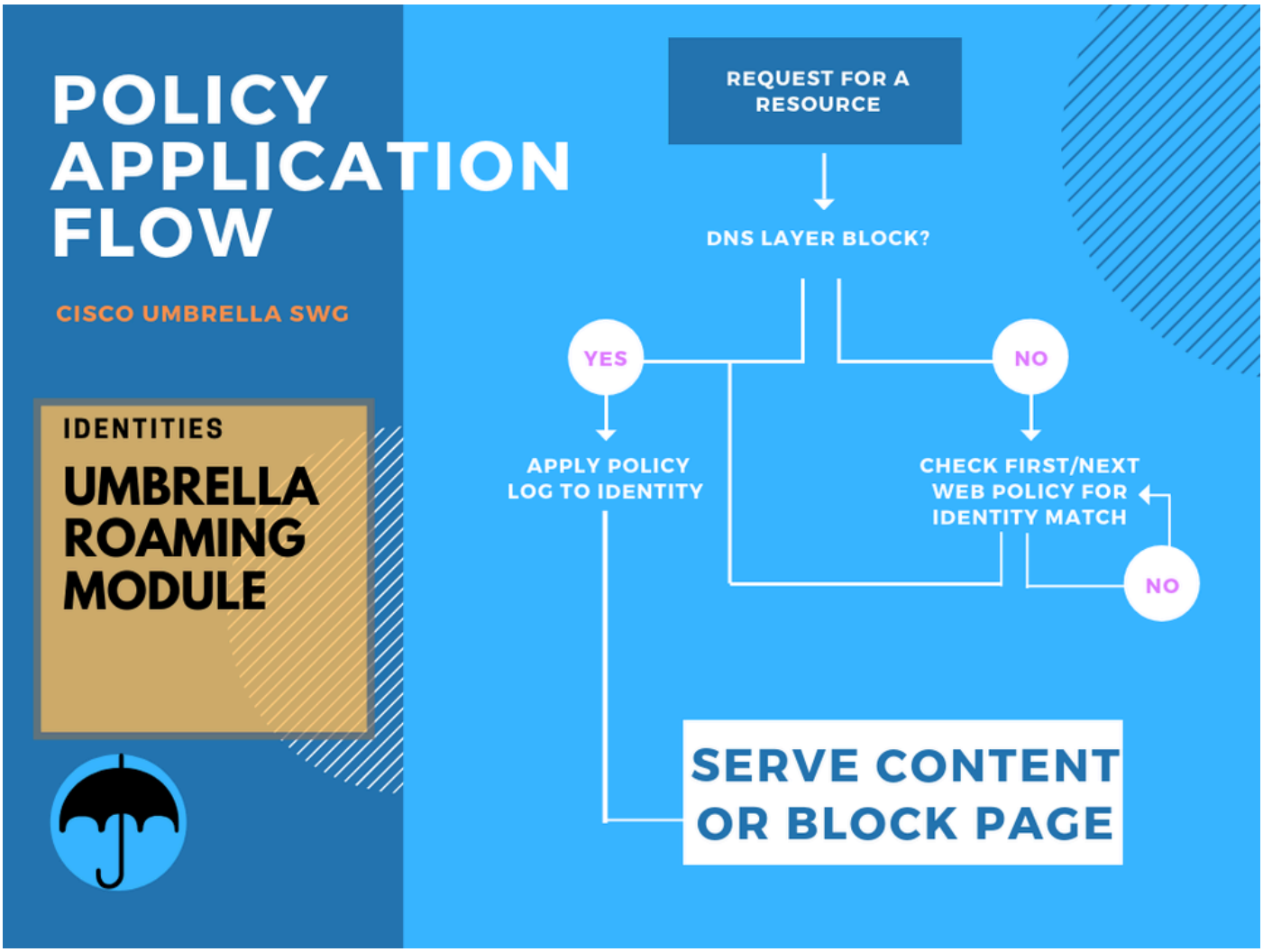
Diagrama de flujo-cdfw.png

Notas importantes sobre las políticas del módulo de seguridad de roaming

Con el módulo de roaming de Umbrella, la política se aplica de manera diferente a las políticas en la red. El módulo de itinerancia no es compatible con las configuraciones de proxy en red o los archivos PAC y sólo admite el caso práctico fuera de la red. Se puede desactivar cuando está en la red.

Mientras se utiliza el módulo de itinerancia con una política SWG, la política DNS se aplica en primer lugar para cualquier bloque, incluidos los bloques de seguridad. Si el resultado de la directiva DNS no es un bloque, se aplica la directiva de proxy. Además, para cualquier tráfico que no sea tráfico HTTP/S, las políticas de DNS se aplican exclusivamente. Por lo tanto, la política se aplica en este orden:

1. Política de DNS (para bloques)
2. política SWG



Flowchart-module.png

¿Desea obtener más información? Eche un vistazo a nuestro vídeo tutorial: Políticas web generales.

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).