Configuración de políticas SIG para acceso remoto para usuarios de conexión segura

Contenido

Introducción

Este documento describe cómo crear políticas SIG para usuarios de Acceso remoto para Secure Connect.

Overview

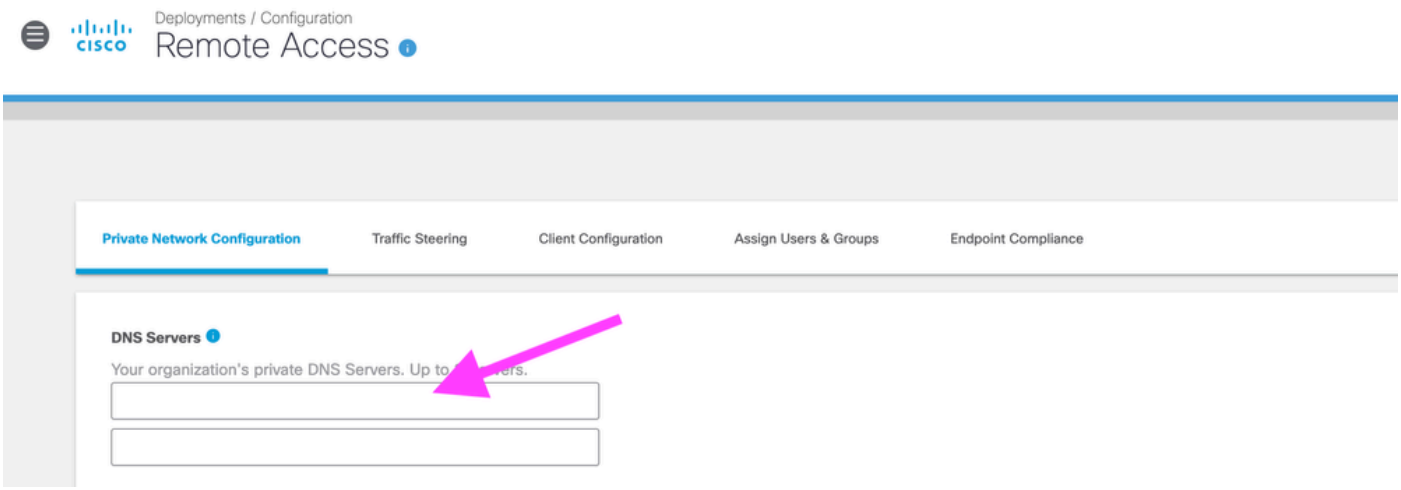
Este artículo de la base de conocimiento se aplica a los clientes que utilizan el paquete Secure Connect, que incluye la funcionalidad de acceso remoto (VPNaaS) en Umbrella.

Los administradores pueden configurar las políticas de Umbrella Firewall, Web y Data Loss para que se apliquen a los usuarios de roaming conectados al acceso remoto mediante AnyConnect.

Políticas de DNS

Es posible enviar consultas de DNS a resolvers de Umbrella (p. ej. 208.67.222.222) a través de la conexión VPN de acceso remoto AnyConnect. Sin embargo, esto no permite la identificación, la política o la generación de informes del tráfico DNS en el panel de Umbrella.

- Esto sólo proporciona resolución DNS y, por lo tanto, no se recomienda normalmente.
- El uso de resolvers DNS externos en la configuración DNS de VPN impide la resolución de zonas DNS internas.

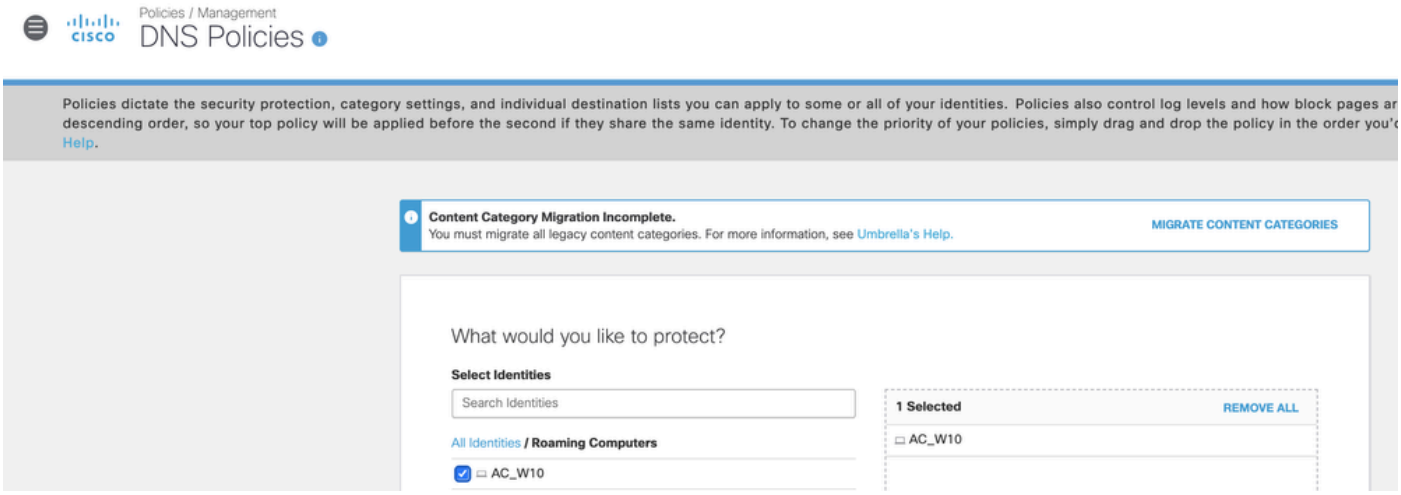


4410210378004

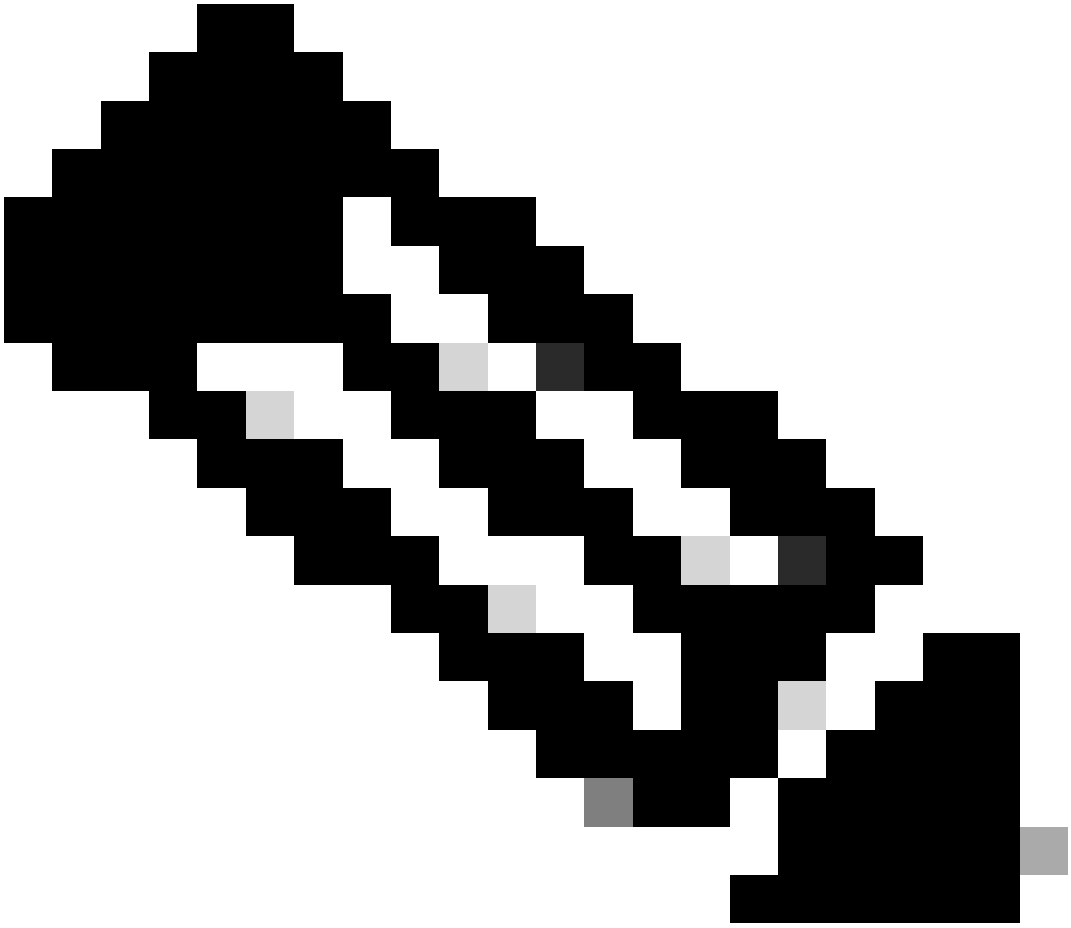
Para agregar identidad, política e informes para consultas DNS, se debe tener en cuenta uno de los tres métodos siguientes:

- (Recomendado) - Implemente el módulo Umbrella AnyConnect Roaming (desde Implementaciones > Equipos Roaming). El tráfico DNS externo se envía directamente a Umbrella con la identidad "Roaming Computer" aplicada. Este módulo también admite la identificación de usuario de AD opcional.
- Reenvíe el tráfico desde el servidor DNS en las instalaciones a Umbrella e identifique el tráfico mediante una identidad de red. Todos los usuarios reciben la misma política/identidad y no hay informes granulares de usuarios.
- Utilice un dispositivo virtual Umbrella en su red en las instalaciones para reenviar el tráfico a Umbrella. Las consultas de DNS se pueden identificar por su dirección interna (dirección IP del grupo VPN). La integración de AD se puede agregar; requiere la instalación de componentes adicionales en las instalaciones.

Este ejemplo muestra cómo se puede configurar una política DNS (Políticas > Políticas DNS) para un cliente AnyConnect individual; esto solo es posible cuando se implementa el módulo Umbrella AnyConnect Roaming Module:



4410210455444



Nota: Cuando se utiliza el módulo Umbrella para AnyConnect, el tráfico DNS se puede enviar opcionalmente dentro o fuera del túnel, según la configuración de túnel dividido.

Políticas de firewall

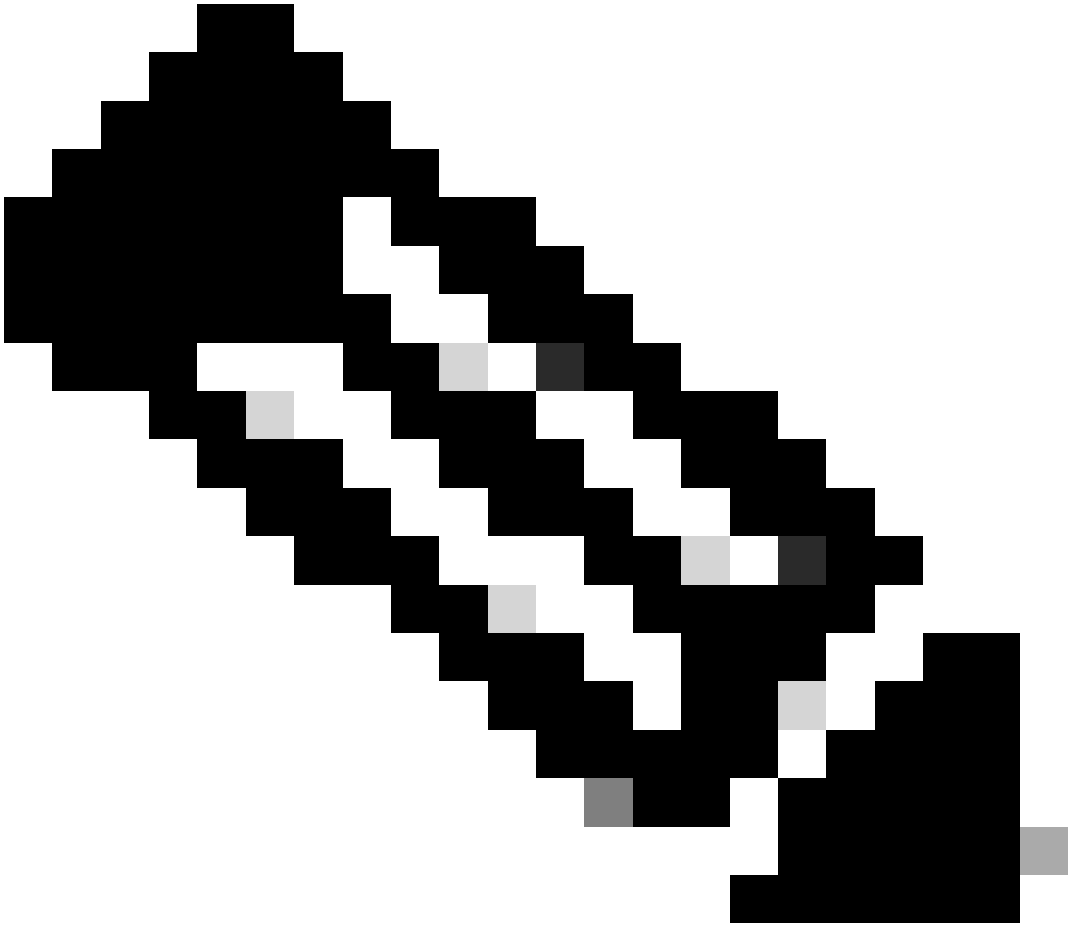
Las políticas de firewall se aplican al tráfico entre los clientes de acceso remoto (AnyConnect) e Internet. Configure las reglas en 'Implementaciones > Política de firewall' según la documentación que se encuentra aquí: Gestione el firewall.

La regla de firewall predeterminada se aplica a los clientes de acceso remoto. Si está creando una directiva específica para usuarios de acceso remoto, puede optar por crear una nueva directiva de firewall y seleccionar "Remote Access Oriid:<ID>" como la identidad del túnel de origen.
La misma política de firewall se aplica a todos los usuarios de acceso remoto.

- Las políticas de firewall no se utilizan para controlar el acceso entre los clientes de RA y las redes privadas/de sucursales. Esto debe controlarse con firewalls en las instalaciones.

- Al igual que todas las reglas de firewall de Umbrella, estas reglas controlan las conexiones salientes de los clientes de acceso remoto. Las conexiones entrantes nunca se permiten.
- La dirección IP de origen para los clientes de acceso remoto siempre se asigna dinámicamente desde el grupo VPN.
    - No se recomienda crear reglas para un equipo específico mediante "IP de origen", ya que la IP se vuelve a asignar dinámicamente
    - La creación de reglas que afectan a los usuarios de un Data Center de acceso remoto específico es posible mediante el uso de un intervalo "Source CIDR". Cada Data Center proporciona un intervalo de grupos de VPN diferente que se configura en la página "Implementaciones > Acceso remoto".

4409322341524



Nota: La identificación por usuario no está disponible para las políticas de firewall.

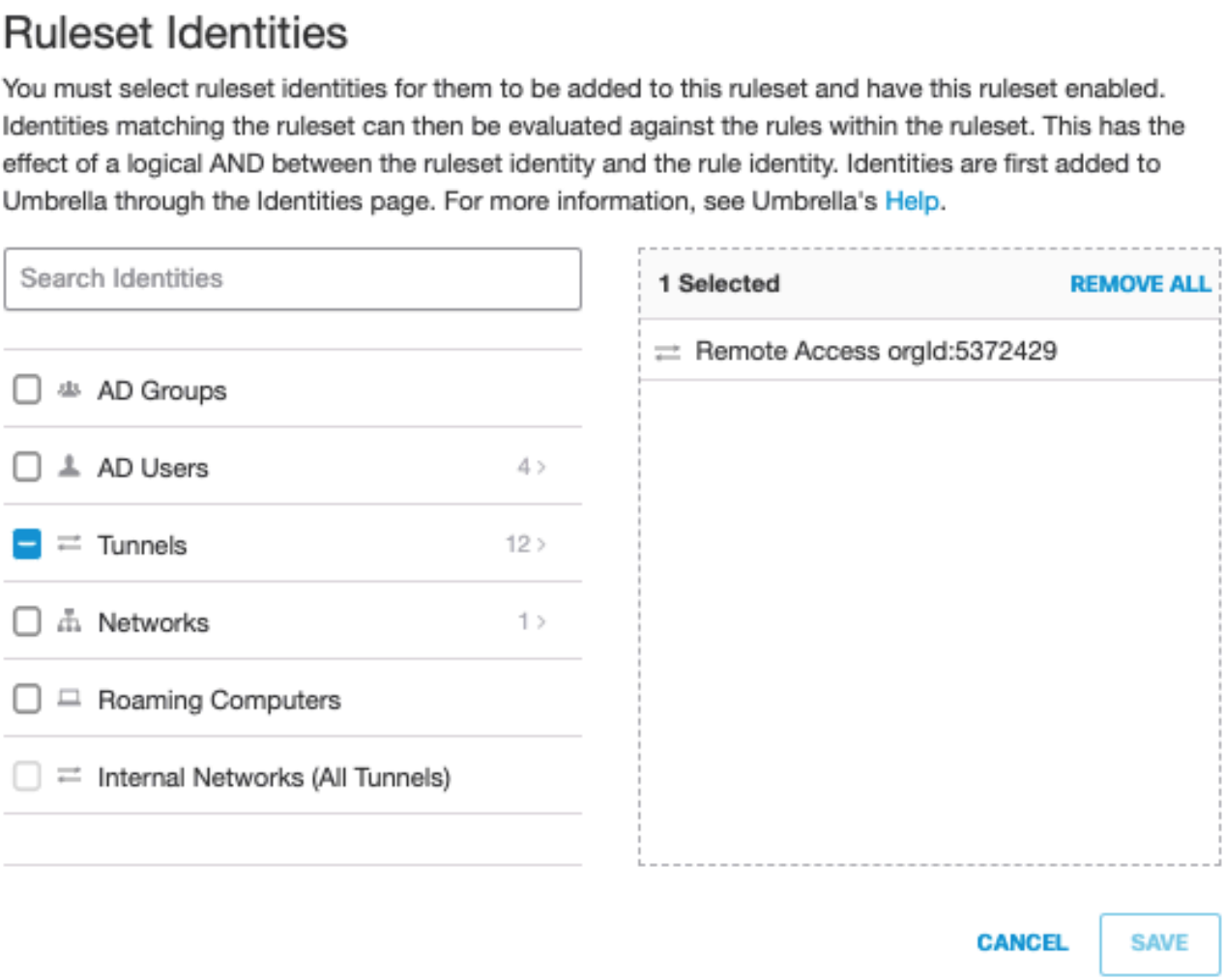
Políticas web

Las directivas Web se aplican al tráfico entre los clientes de acceso remoto (AnyConnect) e Internet. Configure las reglas en 'Implementaciones > Políticas web' según la documentación que se encuentra aquí: Gestionar políticas web.

- Las políticas web no se utilizan para controlar el acceso entre los clientes RA y los servidores web privados/de sucursal. Las políticas web solo se aplican a sitios web externos.

La directiva web predeterminada se aplica a los clientes de acceso remoto. Sin embargo, se recomienda crear un nuevo conjunto de reglas para definir la configuración de seguridad específicamente para los clientes de acceso remoto. Al definir las identidades del conjunto de reglas, elija Remote Access orgid:<ID> de la lista de túneles. La misma política web se aplica a todos los usuarios de acceso remoto.

Después de crear un conjunto de reglas, es posible agregar una regla web a la que se defina el filtrado de categorías de contenido y la configuración de la aplicación.

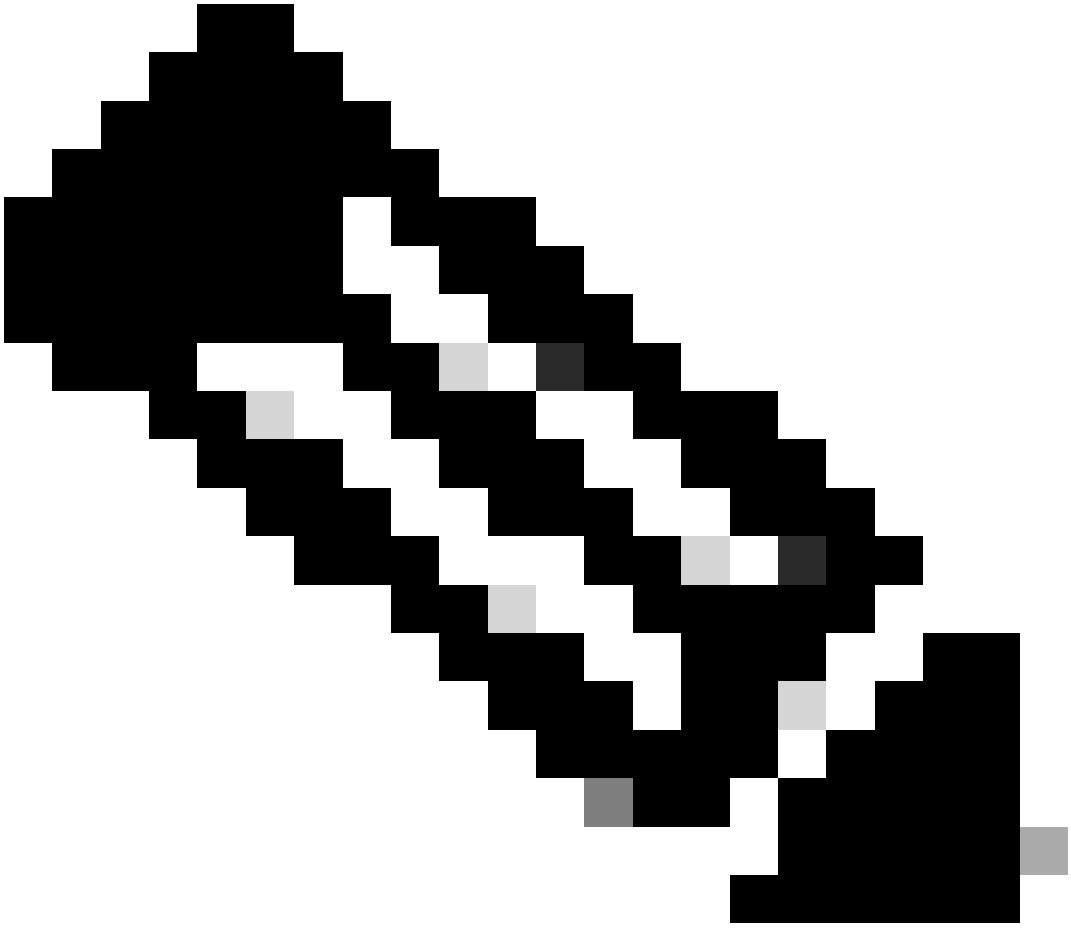


4409322363924

Identificación de usuario web

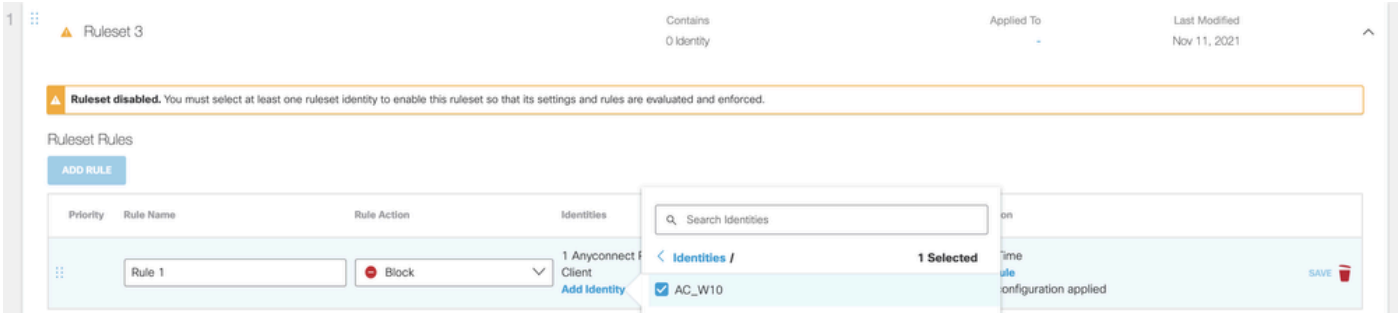
De forma predeterminada, el tráfico de acceso remoto no se puede controlar por usuario o grupo. La misma política se aplica a todo el tráfico RA basado en la identidad "Remote Access Orid". Para agregar la identificación de usuario/grupo, dispone de dos opciones:

- Instale nuestro módulo AnyConnect Umbrella Roaming Security y habilite la función de agente SWG. El agente envía el tráfico web directamente a Umbrella SWG con la identidad "Roaming Computer" aplicada. Este módulo también admite la identificación de usuario de AD opcional.
- Habilite SAML en el conjunto de reglas web que afecta a su identidad de "Id. de acceso remoto". Después de conectarse al acceso remoto, a los usuarios de RA se les pide que se autentiquen a través de SAML por segunda vez cuando generen tráfico del navegador web.



Nota: Cuando se utiliza el módulo Umbrella para AnyConnect, el tráfico SWG se puede enviar opcionalmente dentro o fuera del túnel en función de la configuración de túnel dividido.

Este ejemplo muestra cómo se puede configurar una política DNS (Políticas > Políticas DNS) para un cliente AnyConnect individual - esto solo es posible cuando se implementa el Módulo Umbrella AnyConnect Roaming:

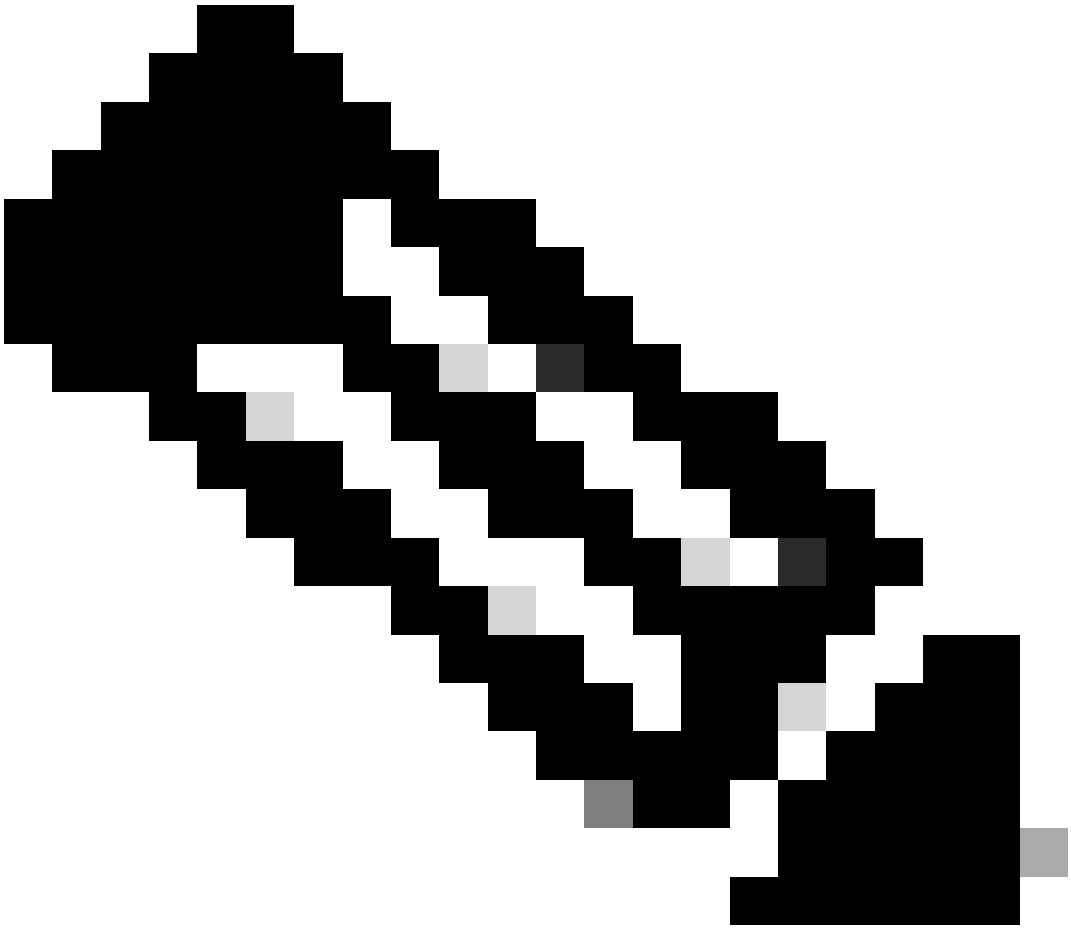


4410210499476

Políticas DLP

Las políticas de pérdida de datos se aplican al tráfico entre los clientes de acceso remoto (AnyConnect) e Internet. Configure las reglas en 'Implementaciones > Políticas de prevención de pérdida de datos' según la documentación que se encuentra aquí: Gestione las políticas de protección de datos.

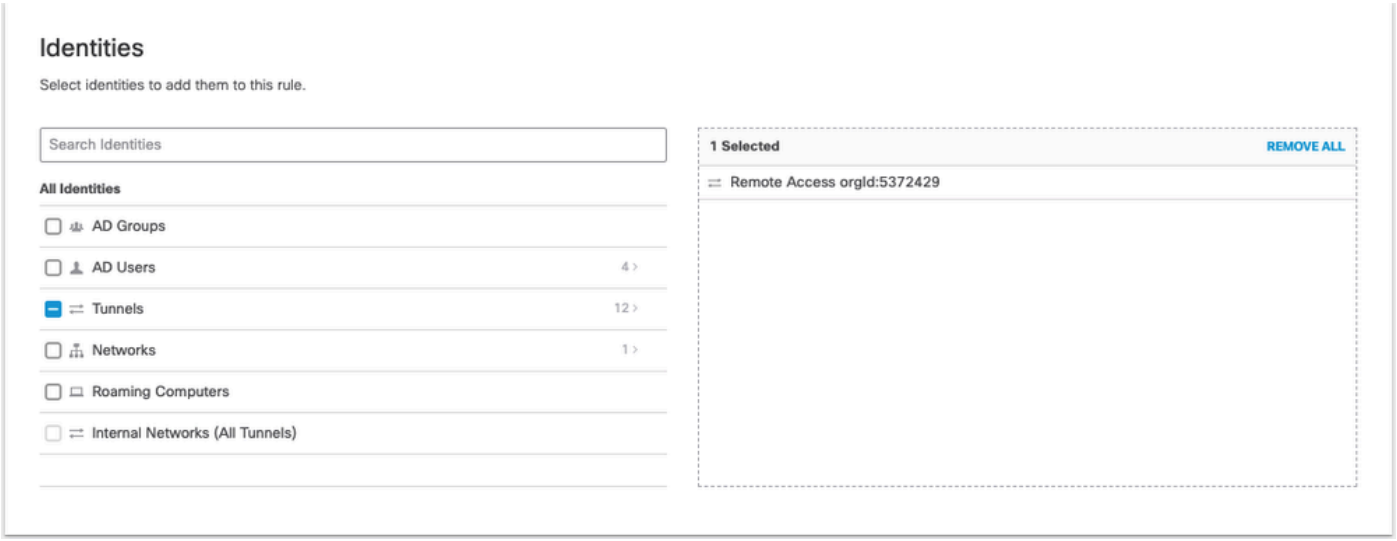
- Las políticas de DLP no se utilizan para controlar el acceso entre los clientes de RA y los servidores web privados/de sucursal. Las políticas de DLP solo se aplican al tráfico de sitios web externos.



Nota: Para que se apliquen las políticas de DLP, primero debe haber creado un conjunto de reglas Web para los usuarios de acceso remoto. El conjunto de reglas web debe tener habilitado el descifrado HTTPS.

Al seleccionar identidades para una regla de protección de datos, elija Remote Access orgid:<ID>. La misma política de protección de datos se aplica a todos los usuarios. Para completar la regla

DLP, también debe seleccionar o definir clasificadores DLP.



4409322428820

Identificación de usuarios de DLP

DLP obtiene la identidad del usuario desde el gateway web seguro (políticas web). Consulte la sección de directivas Web para obtener instrucciones sobre cómo agregar la identificación de usuario.

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).