Implementación de Umbrella DNS para administradores de WLAN de Aruba

Contenido

Introducción

Este documento describe cómo implementar el servicio Umbrella DNS para los administradores de Aruba WLAN.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información de este documento se basa en Cisco Umbrella.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

Aruba Networks cuenta con estas tres líneas de productos de LAN inalámbrica (WLAN) y sistemas operativos para diferentes segmentos de mercado y escenarios de implementación:

- ArubaOS: para grandes organizaciones e implementaciones de alta densidad
- Aruba Instant/InstantOS: para pequeñas y medianas empresas y empresas descentralizadas
- Aruba Instant On: para usuarios domésticos y de pequeñas oficinas

Este artículo proporciona directrices para que los administradores de WLAN de Aruba adopten e implementen el servicio DNS de Umbrella.

Métodos de implementación

Los métodos de implementación dependen de su sistema operativo Aruba y de cómo planee utilizar Umbrella.

Si ejecuta cualquiera de los tres sistemas operativos de Aruba mencionados anteriormente, puede comenzar a implementar Umbrella DNS consultando la guía del usuario de Umbrella. También hay disponibles tutoriales en vídeo.

Si ejecuta Aruba Instant, tiene una opción adicional de utilizar la integración de dispositivos de red Umbrella disponible en InstantOS. Sin embargo, tenga en cuenta que si elige esta opción, no puede ver las direcciones IP internas/privadas de los clientes inalámbricos en la WLAN en los informes de Umbrella, como el informe de búsqueda de actividad. Las consultas de DNS de los clientes se asignan a las identidades de dispositivos de red de los clústeres de puntos de acceso instantáneos en Umbrella, y la información relativa a los clientes individuales no está disponible. Desde la perspectiva de la nube de Umbrella, las consultas de DNS parecen provenir de los clústeres de Instant AP en lugar de los clientes Wi-Fi.

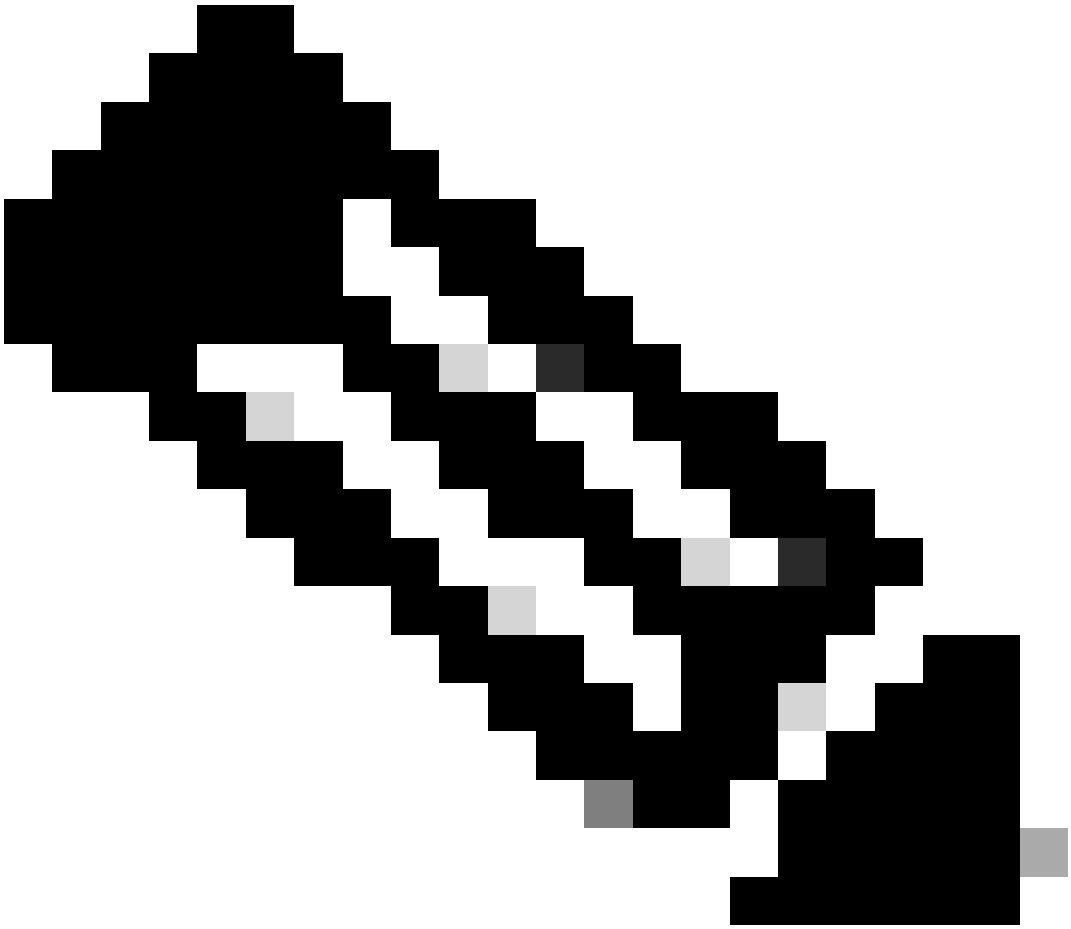
Por lo tanto, si necesita realizar un seguimiento de las consultas de DNS de clientes individuales o personalizar las políticas de DNS para clientes individuales en una WLAN, puede implementar Umbrella mediante los métodos estándar descritos en la guía del usuario de Umbrella DNS (sin utilizar la integración de dispositivos de red a través de Aruba Instant) y considerar la inclusión de los dispositivos virtuales de Umbrella en sus planes de implementación.

Element	Description
AD User	Identified by Virtual Appliance (VA) or Roaming Client (RC).
AD Computer	Identified by VA only.
Internal Network / Umbrella Site	Identified by VA only.
Default Umbrella Site	Traffic on VA with no other identity. Identified by VA only.
Roaming Client	Roaming Client only.
Network	Network Identity based on source IP of the DNS request.

4403300507924

Integración instantánea de Aruba

La integración de dispositivos de red Umbrella (OpenDNS) de Aruba Instant puede ser beneficiosa en entornos en los que todos los clientes Wi-Fi conectados a un clúster de Instant AP están sujetos a una política de Umbrella DNS única y en los que no hay necesidad de revisar las consultas de DNS de los clientes individuales en los informes de Umbrella. En esta sección se explica cómo configurar la integración.



Nota: La integración utiliza una versión antigua de la API de dispositivos de red de Umbrella. La versión antigua no requiere que los clientes generen tokens de API a partir de sus paneles de Umbrella, pero las versiones más recientes sí.

Las API heredadas de Umbrella alcanzaron el fin de su vida útil el 01/09/2023, tras lo cual ya no se proporciona asistencia para la integración. Si tiene algún problema con la integración después de 2023-09-01, complete la sección "Introducción" en la guía de implementación para

implementar Umbrella sin utilizar la integración.

Estos requisitos deben cumplirse para poder utilizar la integración:

- Los AP deben ejecutar la versión 8.10.0.1 o posterior de InstantOS (a partir de mayo de 2022).
- La cuenta de panel de Umbrella utilizada para la integración debe tener el rol de administrador completo.
- La dirección de correo electrónico de la cuenta no se puede asociar a más de un panel de Umbrella. Si no está seguro de si la dirección de correo electrónico solo está asociada a un único panel, puede ponerse en contacto con el servicio de asistencia de Cisco Umbrella para verificarla.
- El inicio de sesión único (SSO) y la autenticación de dos factores (2FA) no se pueden habilitar para la cuenta.
- Si hay un dispositivo de seguridad de red (como un firewall) entre los puntos de acceso e Internet, el dispositivo debe permitir conexiones sin filtrar ni inspeccionar a 208.67.220.220, 208.67.222.222, 67.215.92.210 y 146.112.255.152/29 (.152 ~ .159).

Configuración

En un nivel superior, hay cuatro pasos de configuración para habilitar la integración:

1. Establezca un nombre para el clúster de AP

2. Introduzca las credenciales de la cuenta

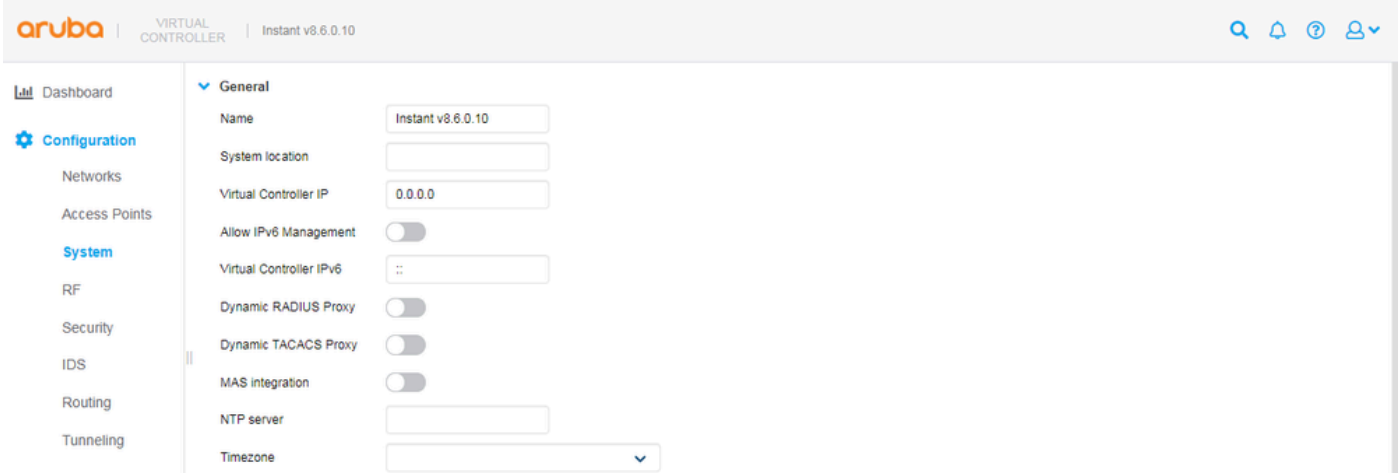
3. Interceptar consultas DNS

4. Aplicar la política DNS

Establecer un nombre para el clúster de PA

Cuando un clúster instantáneo se registra correctamente en un panel de Umbrella por primera vez, se agrega una entrada de dispositivo de red al panel de Umbrella en Implementaciones > Dispositivos de red. El nombre de dispositivo de una nueva entrada proviene del nombre del sistema configurado en el controlador virtual de un clúster.

Para configurar el nombre del sistema en un controlador virtual Instant, navegue hasta Configuration > System.



4404011628308

Tenga en cuenta que el valor del nombre se copia sólo una vez durante el registro inicial. Si después se cambia el nombre de un sistema/dispositivo en el lado Instant (Instante) o Umbrella (Paraguas), deberá actualizar manualmente el nombre en el otro lado.

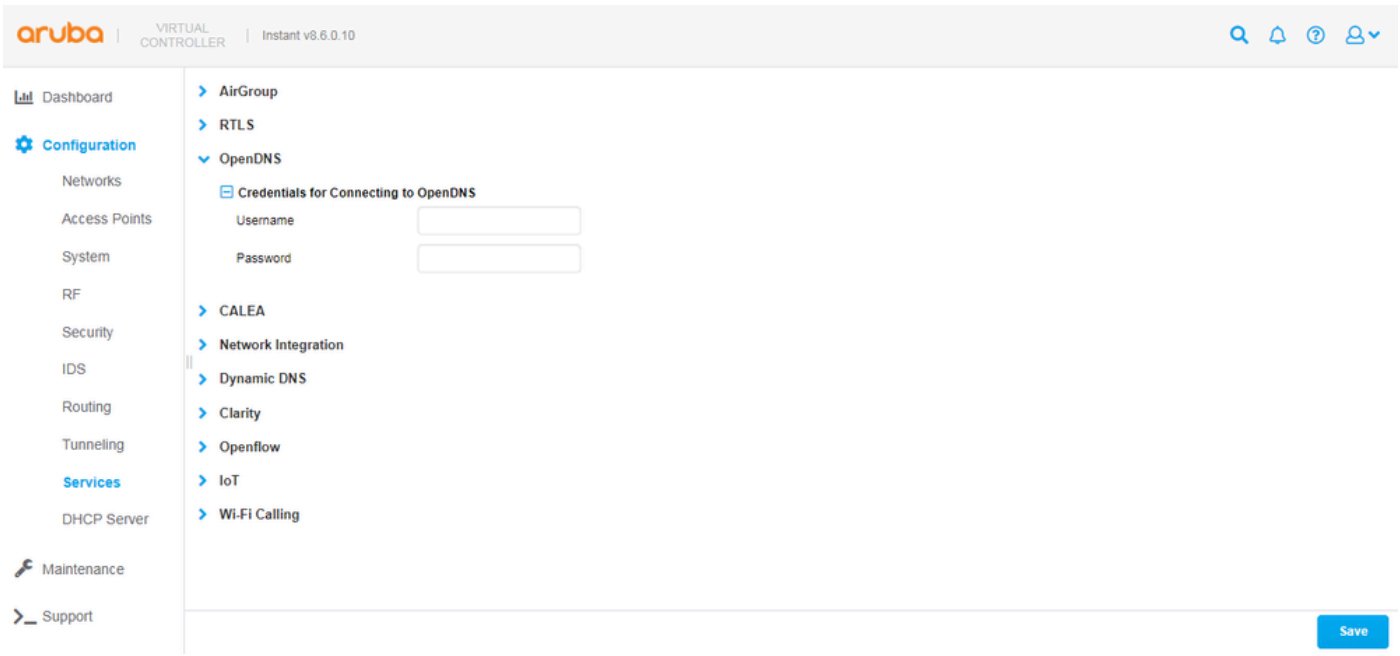
Introducir credenciales de cuenta

Si se cumplen los requisitos enumerados en la sección Requisitos previos, puede agregar un clúster instantáneo al panel de Umbrella como dispositivo de red. Para hacerlo desde el controlador virtual de un clúster:

1. Vaya a Configuration > Services > OpenDNS.

2. Introduzca las credenciales de conexión de una cuenta de Umbrella.

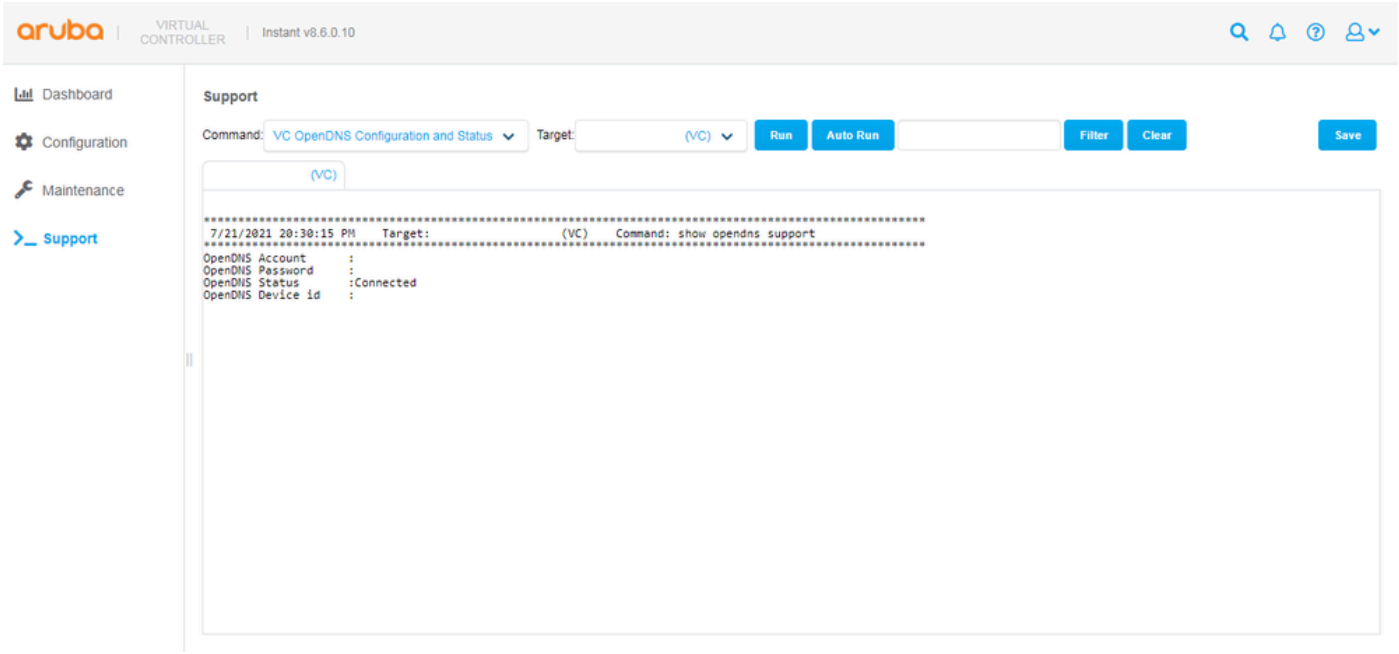
3. Seleccione Guardar.



4404019266196

Si el controlador virtual (VC) se conecta correctamente a Umbrella, puede ver el estado Connected cuando navega hasta Support y ejecuta el comando "VC OpenDNS Configuration and Status" (`show openns support`).

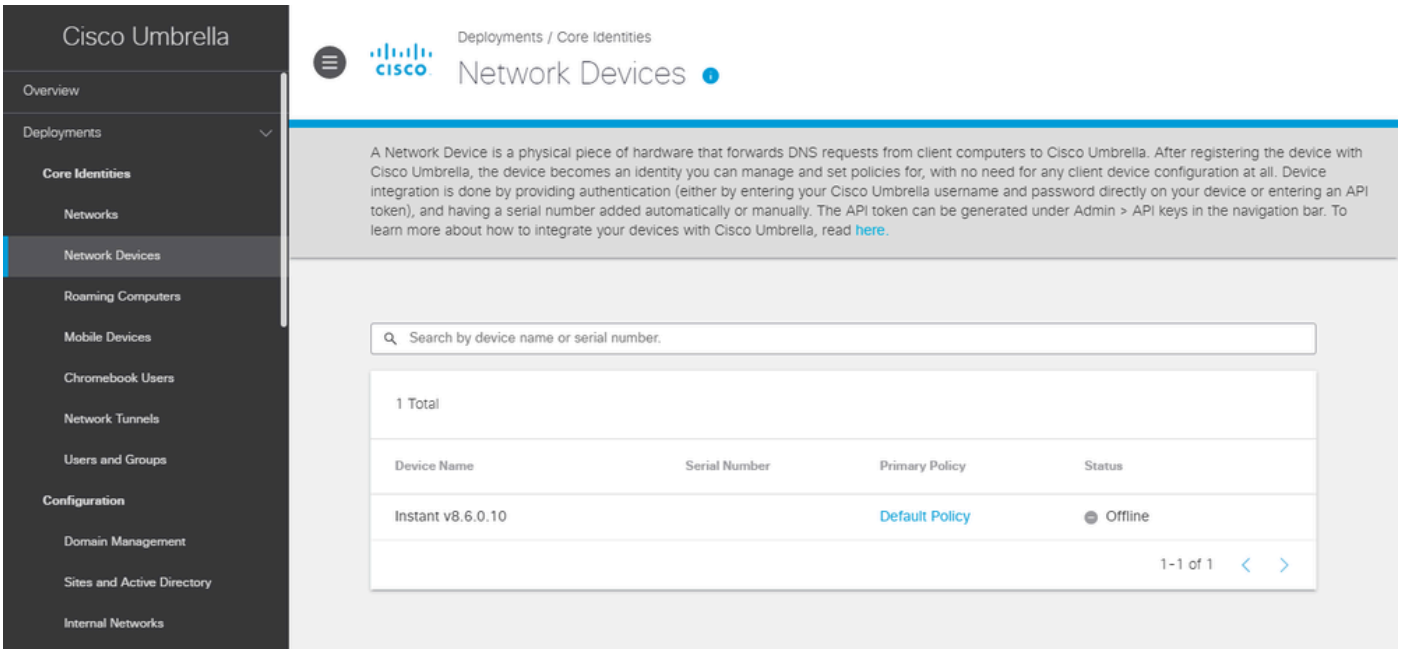
También puede ver un ID de dispositivo, que genera Umbrella cuando se crea un nuevo dispositivo de red y se guarda en la configuración de Instant VC. Esta última parte es importante. Dado que cada clúster Instant necesita tener un ID de dispositivo de red Umbrella único, el ID de dispositivo no se debe copiar de la configuración de un clúster a otro. Un ID de dispositivo válido normalmente tiene 16 dígitos.



4404019268116

Si el resultado del comando muestra un estado Not connected, puede intentar averiguar por qué ejecutando los comandos "AP Tech Support Dump" (`show tech-support`) y "AP Tech Support Dump Supplemental" (`show tech-support suplemental`), y luego buscar "opendns" en los registros. Los resultados de los comandos también se pueden compartir con Aruba TAC para fines de resolución de problemas.

Si todo funciona correctamente, puede ver una nueva entrada en el panel de Umbrella en Implementaciones > Dispositivos de red, donde puede buscar un clúster de Instant AP por su nombre o eliminar una entrada existente si desea generar un nuevo ID de dispositivo.



4404011658516

Interceptar consultas DNS

Tras confirmar que un clúster se ha agregado correctamente al panel de Umbrella como dispositivo de red, puede configurar el clúster para que comience a interceptar consultas DNS enviadas desde clientes inalámbricos (que están conectados a los puntos de acceso del clúster). Una vez configurado, independientemente de las direcciones IP del servidor DNS que se hayan configurado en las NIC de los clientes inalámbricos, el clúster puede interceptar las consultas DNS de los clientes y reenviarlas a los resolvers de difusión por proximidad de Umbrella en 208.67.220.220 y 208.67.222.222.

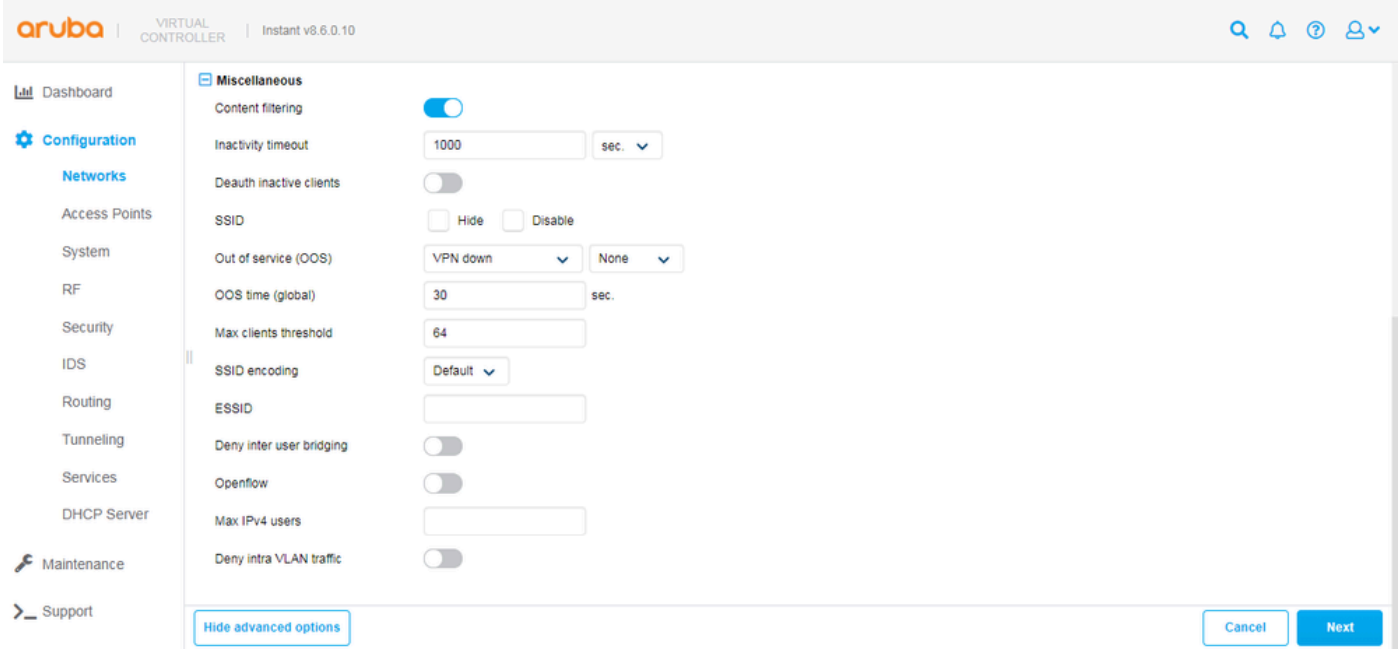
Para interceptar consultas DNS:

1. Navegue hasta el controlador virtual de un clúster en Configuration > Networks.

2. Seleccione una red inalámbrica.

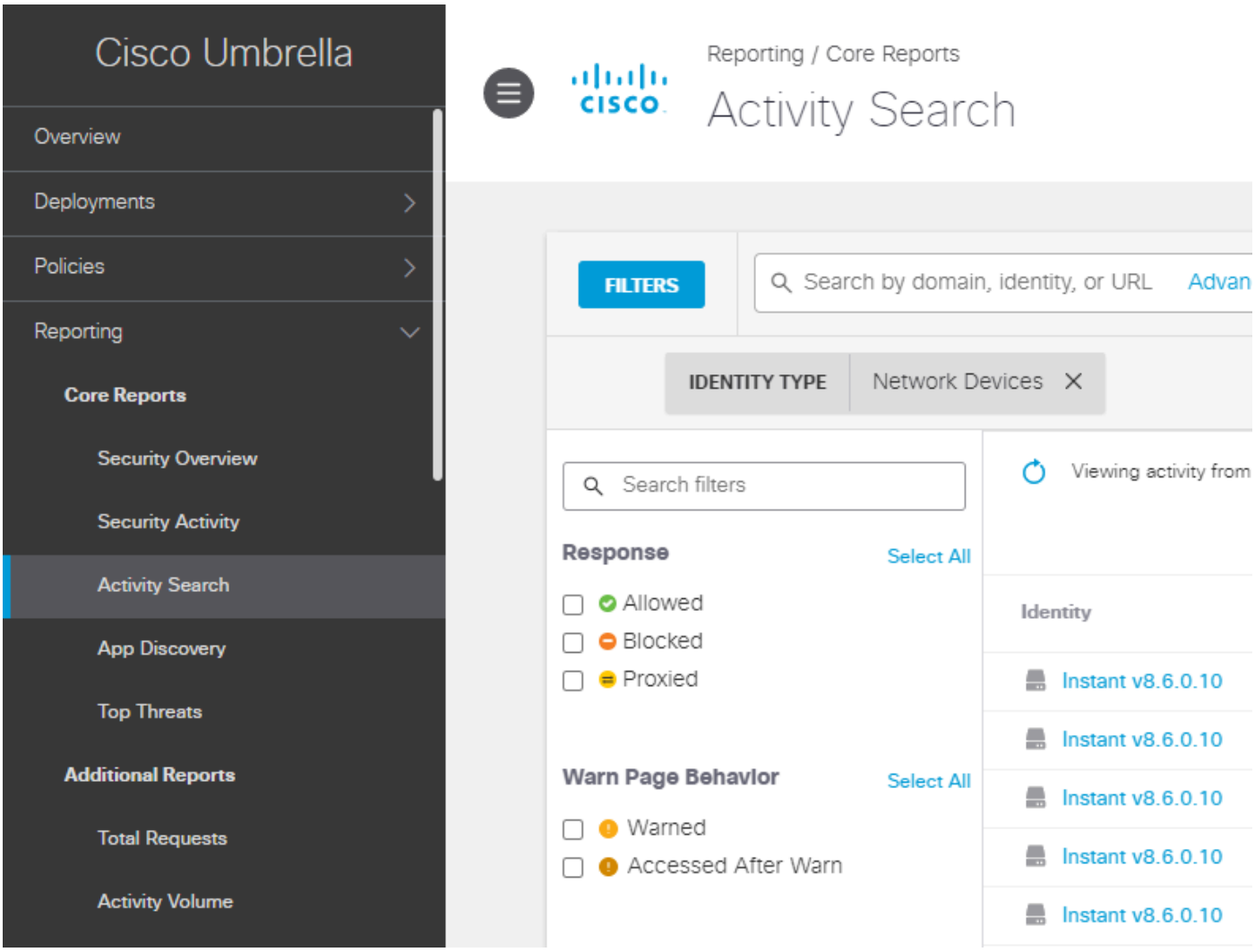
3. Edite la red, seleccione Show advanced options y desplácese a la sección Miscellaneous.

4. Active la opción Filtrado de Contenido y siga seleccionando Siguiente hasta que pueda pulsar el botón Finalizar para guardar el cambio.



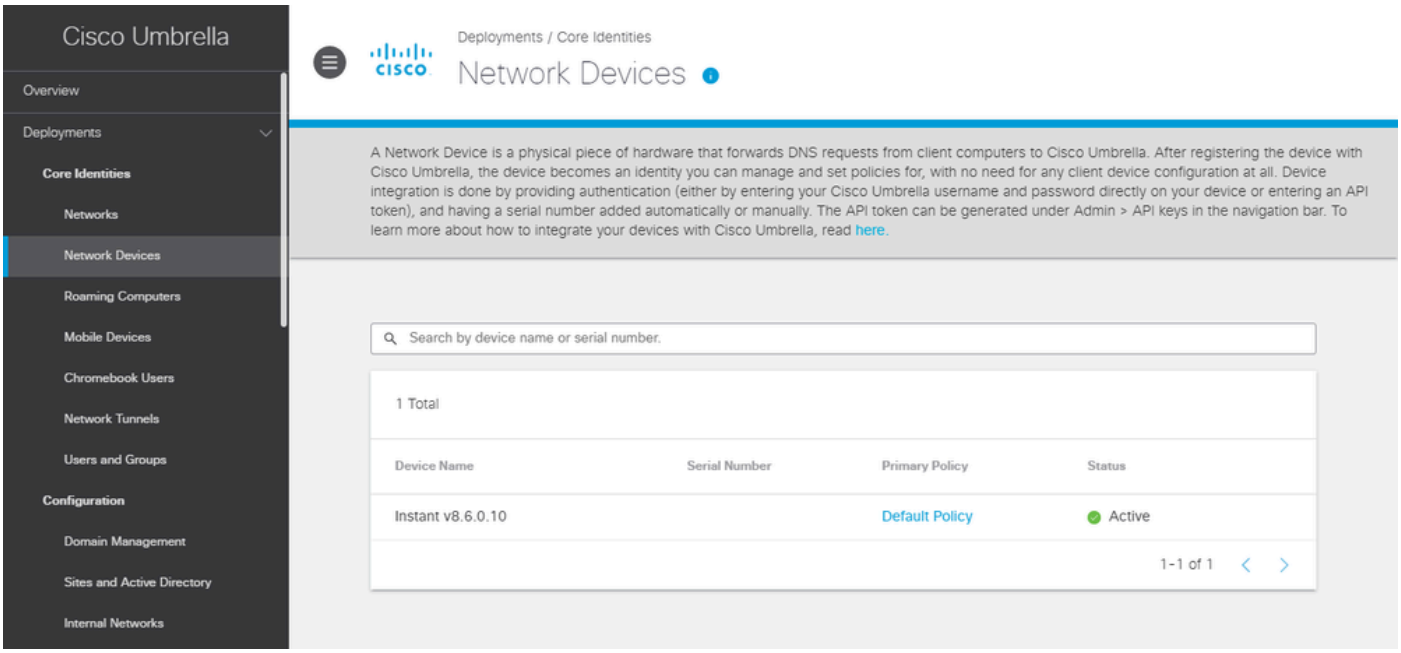
4404011668500

Después de activar la opción, puede empezar a ver las consultas DNS en el panel de Umbrella en Reporting > Activity Search. La identidad de las consultas se puede asignar a un nombre de dispositivo de red, que suele ser el nombre del sistema configurado en el controlador virtual de un clúster de AP. Tenga en cuenta que las consultas pueden tardar algún tiempo (unos 15 minutos) en procesarse y mostrarse en la GUI del panel.



4404011721620

En el panel general, en Implementaciones > Dispositivos de red, un dispositivo puede tardar hasta 24 horas en cambiar a un estado activo/en línea. El estado de un dispositivo de red indica simplemente si el dispositivo interceptó las consultas DNS y las reenvió a Umbrella en las 24 horas anteriores, y no influye en la forma en que el dispositivo se comunica con Umbrella. Un estado fuera de línea/inactivo puede significar simplemente que ningún cliente inalámbrico se conectó a un clúster de AP en las últimas 24 horas y no puede impedir que el clúster utilice el servicio Umbrella.

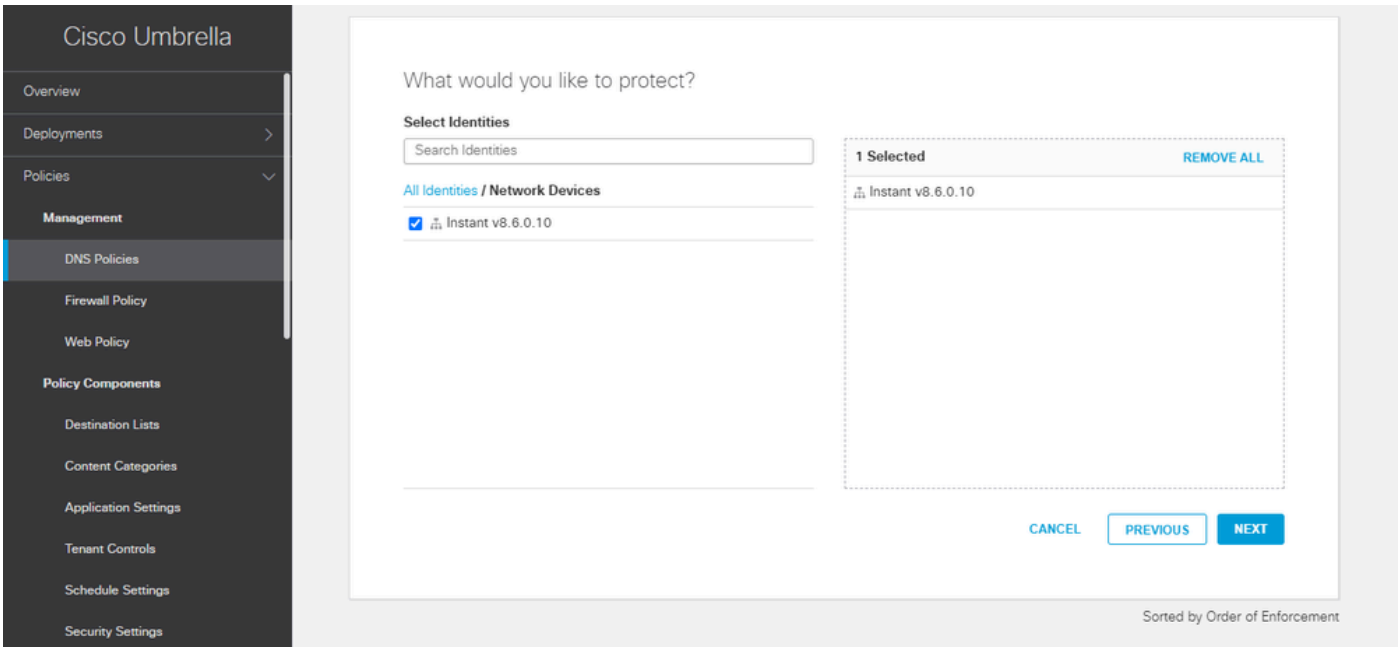


4404011756308

Aplicar política DNS

En Umbrella, la "Política predeterminada" incluye automáticamente todas las identidades (como los dispositivos de red) agregadas a un panel. No es necesario crear políticas DNS adicionales si todos los clústeres de AP de la implementación pueden estar sujetos a la misma política. Si este es su caso, pase a la siguiente sección.

Como alternativa, si desea aplicar una política personalizada a un dispositivo de red específico, debe agregar una nueva política en el panel de Umbrella, en Políticas > Todas las políticas (Políticas DNS), y seleccionar el dispositivo de red en la política.



4404011773588

Cuando hay más de una política en la página Políticas DNS (todas las políticas), las políticas se

evalúan de arriba a abajo en base a la primera coincidencia. Para obtener más información, consulte la documentación de precedencia de políticas y las prácticas recomendadas para definir la documentación de políticas.

DNS interno

En un entorno en el que existan servidores DNS internos y desee reenviar consultas DNS de determinados dominios (internos) a los servidores DNS internos, puede utilizar la función Dominios de empresa en Instant.

Las consultas DNS pueden continuar siendo interceptadas por el clúster AP después de que se habilite la función, excepto que las consultas para los dominios especificados ya no se pueden reenviar a Umbrella. En su lugar, se pueden reenviar a las direcciones IP del servidor DNS configuradas originalmente en las NIC de los clientes inalámbricos (como a través de DHCP). La función es similar a la funcionalidad de Dominios internos disponible en los métodos de implementación estándar de Umbrella (con appliances virtuales), donde no se utiliza la integración de Aruba Instant.

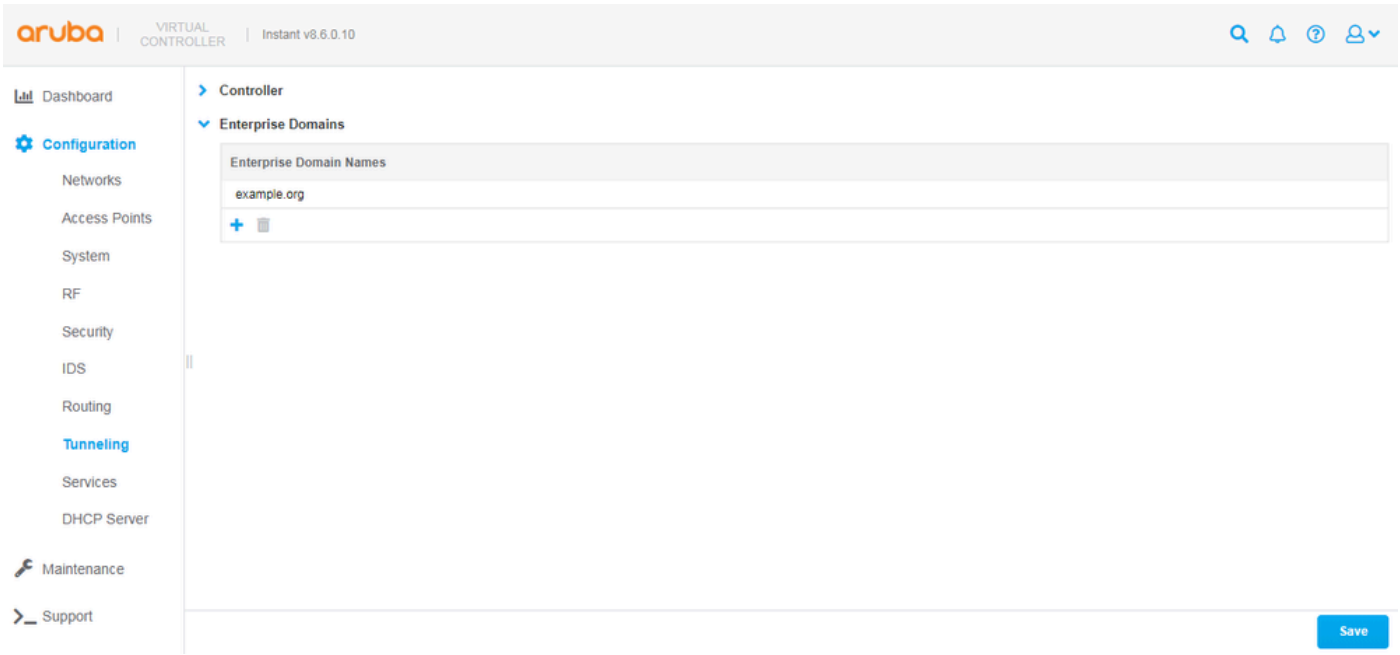
Para configurar la función en un controlador virtual Instant:

1. Acceda a Configuración > Tunelización > Dominios de Empresa.

2. Agregue o elimine dominios de la lista Nombres de dominio de empresa.

3. Seleccione Guardar.

Hay un comodín implícito para cualquier dominio agregado a la lista, por lo que example.org implica *.example.org.



4404238114452

Verificación

Tanto si ha implementado Umbrella en su WLAN mediante los métodos estándar a los que se hace referencia en la sección "Descripción general de la implementación" de esta guía, como si ha implementado la integración descrita en la sección "Aruba Instant Integration", puede verificar que los clientes inalámbricos estén utilizando Umbrella DNS navegando a https://welcome.umbrella.com/ desde uno de los clientes. A continuación, verá una marca de verificación verde similar a la captura de pantalla que se muestra en la documentación de Umbrella.

4404011960212

Como alternativa, puede verificar esto ejecutando este comando en el símbolo del sistema de un cliente inalámbrico.

```
nslookup -type=txt debug.opendns.com.
```

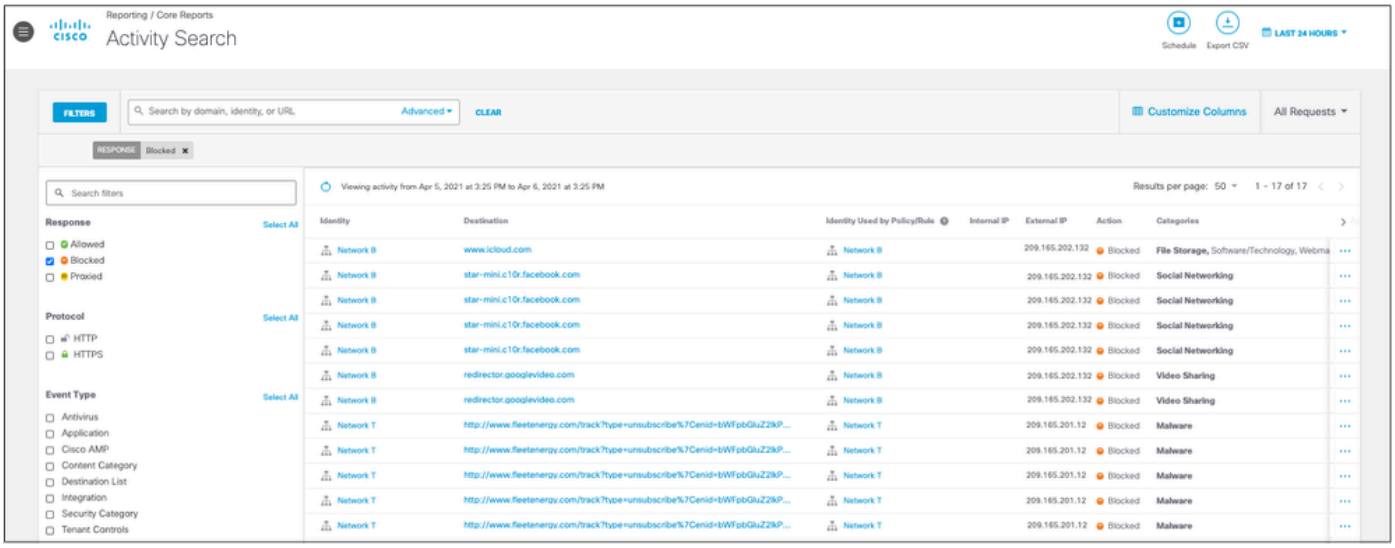
Puede ver una salida con un número de líneas de texto, similar a esta captura de pantalla:

```
anthony@ubuntu:~/Desktop$ nslookup -type=txt debug.opendns.com.
Server:         127.0.1.1
Address:        127.0.1.1#53

Non-authoritative answer:
debug.opendns.com       text = "server 7.pao"
debug.opendns.com       text = "organization id [redacted]
debug.opendns.com       text = "appliance id [redacted]
debug.opendns.com       text = "host id [redacted]
debug.opendns.com       text = "user id [redacted]
debug.opendns.com       text = "remoteip [redacted]
debug.opendns.com       text = "flags [redacted]
debug.opendns.com       text = "id [redacted]
debug.opendns.com       text = "source [redacted]
debug.opendns.com       text = "fw: flags [redacted]
debug.opendns.com       text = "fw: id [redacted]
debug.opendns.com       text = "fw: source [redacted]

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

En el resultado del comando, puede ver el ID de organización de su panel de Umbrella en la línea "orgid" o "organization id", y si utiliza la integración instantánea, puede ver la línea "device" adicional que contiene un ID de dispositivo.

Para revisar las consultas de DNS en el panel de Umbrella, vaya a Informes > Búsqueda de actividad. Tenga en cuenta que las consultas pueden tardar algún tiempo (unos 15 minutos) en mostrarse en la GUI del panel. Encontrará instrucciones sobre cómo utilizar la búsqueda de actividad en la documentación de Umbrella.



4404019393044

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).