Implante o DNS Umbrella para administradores de WLAN da Aruba

Contents

Introdução

Este documento descreve como implantar o serviço Umbrella DNS para administradores de WLAN da Aruba.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

A Aruba Networks tem essas três linhas de produtos e sistemas operacionais de LAN sem fio (WLAN) para diferentes segmentos de mercado e cenários de implantação:

- ArubaOS: para grandes empresas e implantações de alta densidade
- Aruba Instant / InstantOS: para empresas de pequeno a médio porte e empresas distribuídas
- Aruba Instant Aceso: para usuários domésticos e de pequenos escritórios

Este artigo fornece diretrizes para que os administradores de WLAN da Aruba adotem e implantem o serviço Umbrella DNS.

Métodos de implantação

Os métodos de implantação dependem do seu sistema operacional Aruba e de como você planeja usar o Umbrella.

Se você executar qualquer um dos três sistemas operacionais da Aruba mencionados anteriormente, poderá começar a implantar o Umbrella DNS consultando o guia do usuário do Umbrella. Tutoriais em vídeo também estão disponíveis.

Se você executar o Aruba Instant, terá uma opção adicional de usar a integração do dispositivo de rede Umbrella disponível no InstantOS. No entanto, observe que, se você escolher essa opção, não poderá ver os endereços IP internos/privados dos clientes sem fio na WLAN nos relatórios do Umbrella, como o relatório de pesquisa de atividades. As consultas DNS de clientes são mapeadas para as identidades de dispositivo de rede dos clusters de AP instantâneo no Umbrella, e as informações sobre os clientes individuais não estão disponíveis. Da perspectiva da nuvem Umbrella, as consultas de DNS podem parecer vir dos clusters de AP instantâneo, em vez dos clientes Wi-Fi.

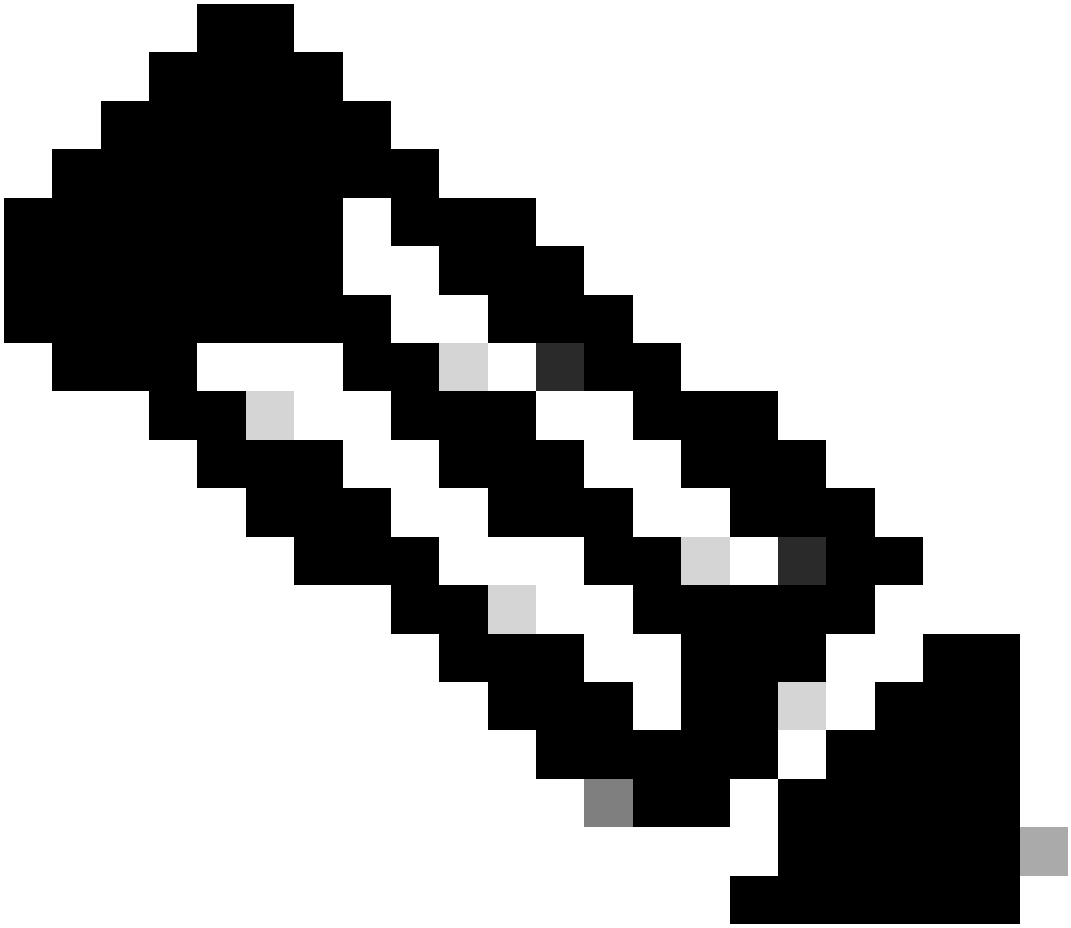
Como tal, se você tem um requisito para rastrear consultas DNS de clientes individuais ou para ajustar políticas DNS para clientes individuais em uma WLAN, você pode implantar o Umbrella através de métodos padrão descritos no guia do usuário do Umbrella DNS (sem usar a integração de dispositivo de rede através do Aruba Instant), e considerar a inclusão de dispositivos virtuais do Umbrella em seus planos de implantação.

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

Integração instantânea Aruba

A integração do dispositivo de rede Umbrella (OpenDNS) da Aruba Instant pode ser benéfica em ambientes onde todos os clientes Wi-Fi conectados a um cluster Instant AP estão sujeitos a uma política de DNS Umbrella única, e onde não há necessidade de revisar consultas DNS de clientes individuais nos relatórios Umbrella. Esta seção explica como configurar a integração.



Note: A integração usa uma versão antiga da API de dispositivos de rede da Umbrella. A versão legada não exige que os clientes gerem tokens de API a partir de seus painéis Umbrella, mas as versões mais recentes o fazem.

As APIs herdadas da Umbrella chegaram ao fim da vida útil em 01/09/2023, após o qual o suporte não será mais fornecido para a integração. Se você encontrar algum problema com a integração após 2023-09-01, preencha a seção "Introdução" no guia de implantação para implantar o Umbrella sem usar a integração.

Estes requisitos precisam ser atendidos para usar a integração:

- Os APs precisam executar o InstantOS versão 8.10.0.1 ou mais recente (a partir de maio de 2022).
- A conta do painel do Umbrella usada para a integração precisa ter a função de Administrador Completo.
- O endereço de email da conta não pode ser associado a mais de um painel do Umbrella. Se não tiver certeza se o endereço de e-mail está associado apenas a um único painel, você pode entrar em contato com o Suporte do Cisco Umbrella para verificar.
- Não é possível habilitar o logon único (SSO) e a autenticação de dois fatores (2FA) para a conta.
- Se houver um dispositivo de segurança de rede (como um firewall) entre APs e a Internet, o dispositivo precisa permitir conexões não filtradas e não inspecionadas a 208.67.220.220, 208.67.222.222, 67.215.92.210 e 146.112.255.152/29 (0,152 ~ 0,159).

Configuração

Em um alto nível, há quatro etapas de configuração na habilitação da integração:

1. Defina um nome para o cluster AP

2. Informe as credenciais da conta

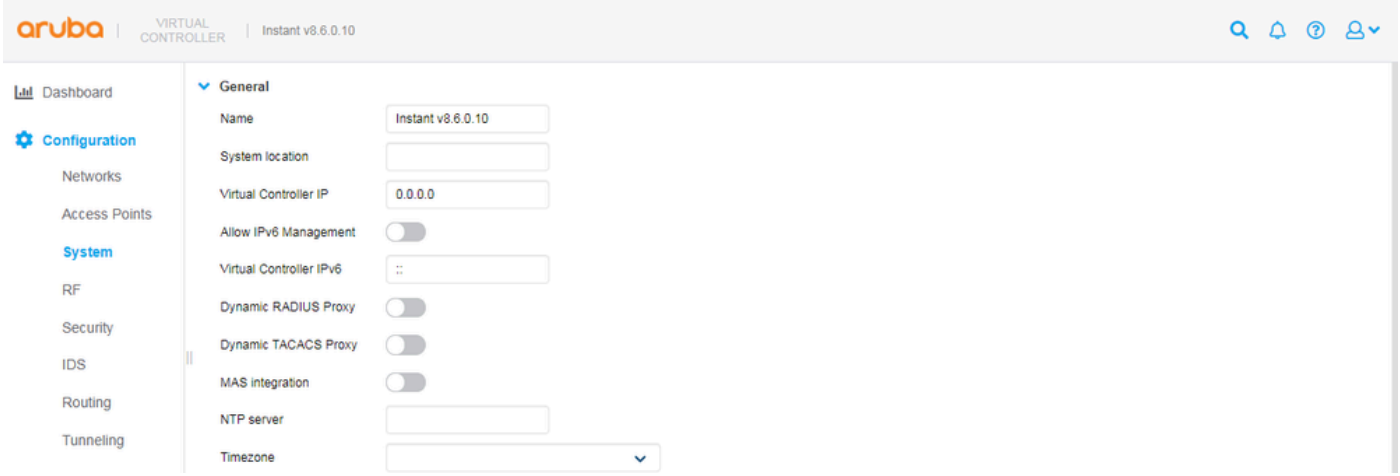
3. Interceptar consultas DNS

4. Aplicar política de DNS

Defina um nome para o cluster AP

Quando um cluster instantâneo se registra com êxito em um painel do Umbrella pela primeira vez, uma entrada de dispositivo de rede é adicionada ao painel do Umbrella em Implantações > Dispositivos de rede. O nome do dispositivo de uma nova entrada vem do nome do sistema configurado em um controlador virtual do cluster.

Para definir o nome do sistema em um controlador virtual instantâneo, navegue para Configuração > Sistema.



4404011628308

Observe que o valor do nome é copiado apenas uma vez durante o registro inicial. Se um nome de sistema/dispositivo for alterado no lado Instantâneo ou Guarda-chuva posteriormente, você deverá atualizar manualmente o nome no outro lado.

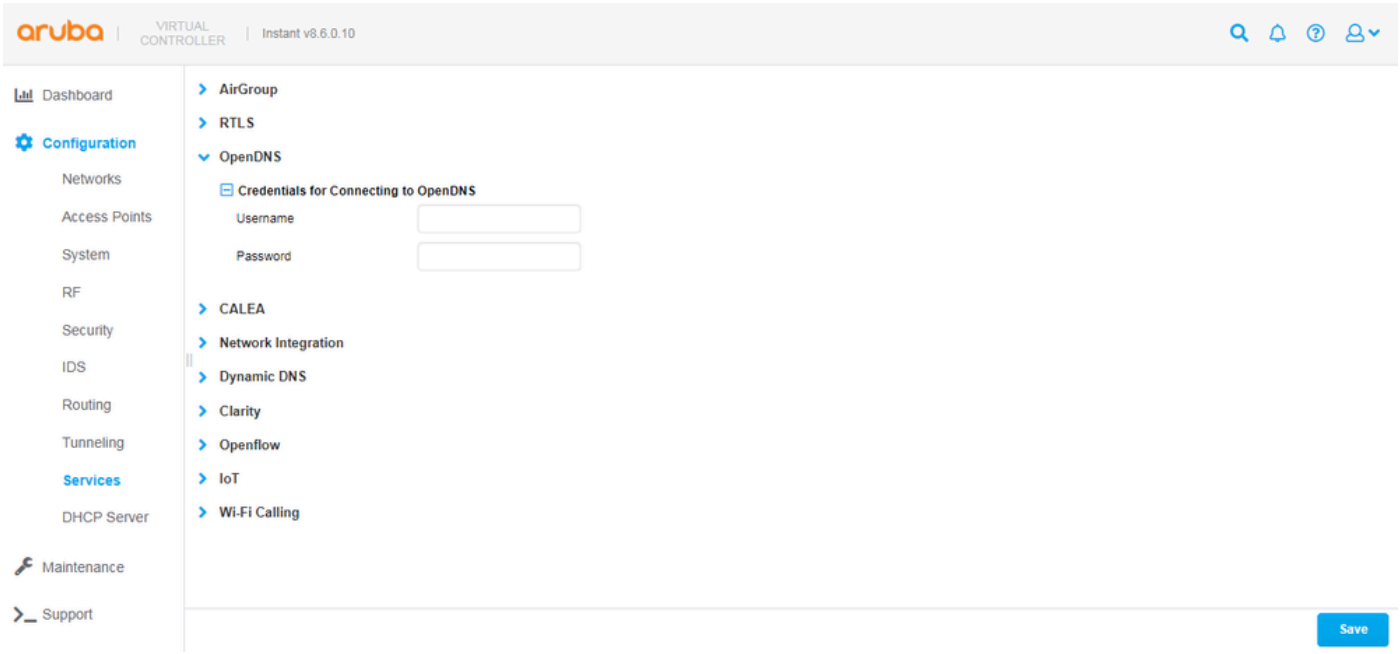
Inserir Credenciais da Conta

Se os requisitos listados na seção Pré-requisitos forem atendidos, você poderá adicionar um cluster Instantâneo ao painel do Umbrella como um dispositivo de rede. Para fazer isso a partir do controlador virtual de um cluster:

1. Navegue até Configuration > Services > OpenDNS.

2. Informe as credenciais de login de uma conta Umbrella.

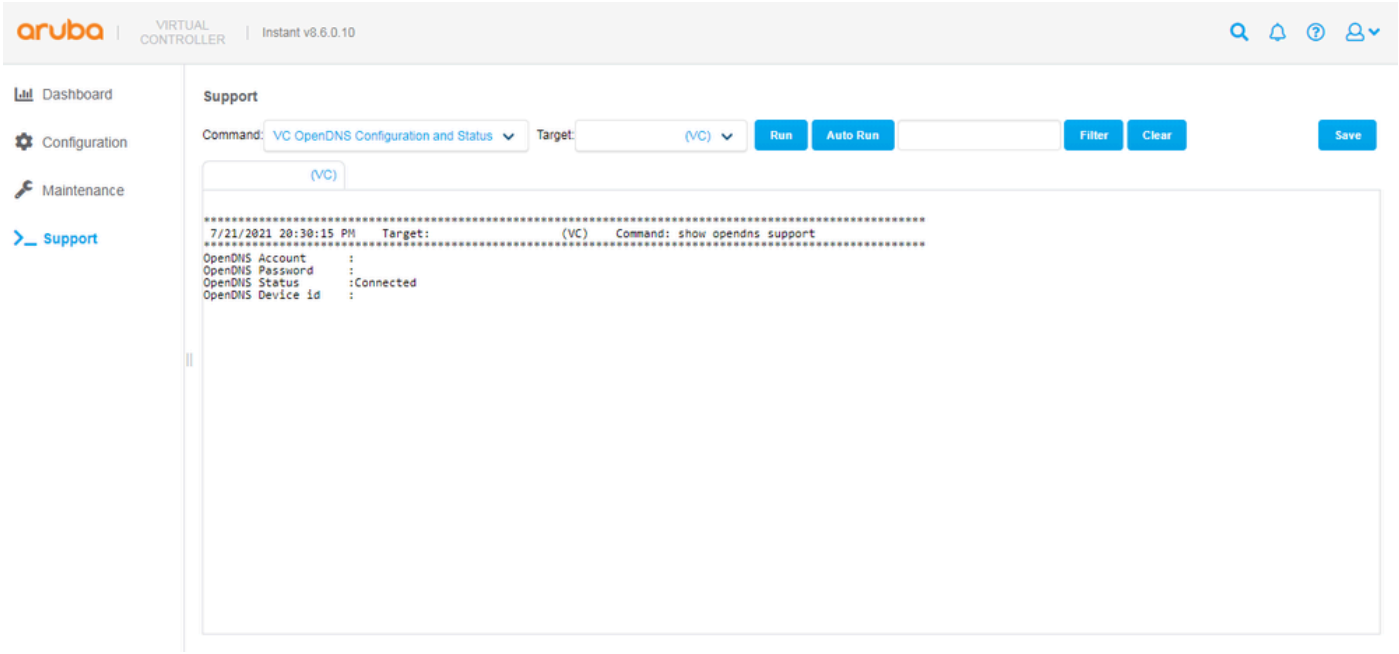
3. Selecione Salvar.



4404019266196

Se o controlador virtual (VC) se conectar com êxito ao Umbrella, você poderá ver o status Connected quando navegar para Support e executar o comando "VC OpenDNS Configuration and Status" (`show opendns support`).

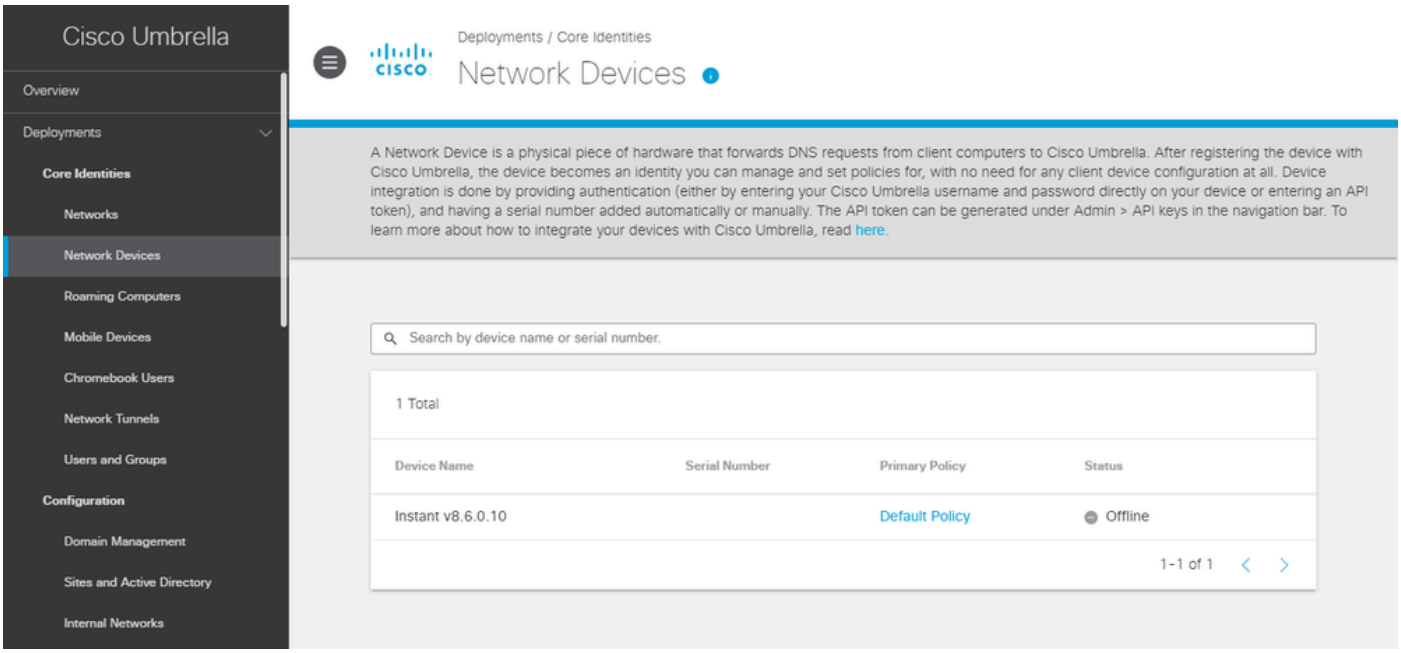
Você também pode ver uma ID de dispositivo, que é gerada pelo Umbrella quando um novo dispositivo de rede é criado e salvo na configuração do Instant VC. A última parte é importante. Como cada cluster instantâneo precisa ter uma ID de dispositivo de rede Umbrella exclusiva, a ID de dispositivo não deve ser copiada da configuração de um cluster para outra. Um ID de dispositivo válido normalmente tem 16 dígitos.



4404019268116

Se a saída do comando mostrar o status Not connected, você poderá tentar descobrir por que ao executar os comandos "AP Tech Support Dump" (`show tech-support`) e "AP Tech Support Dump Supplemental" (`show tech-support suplemental`) e procurar "opendns" nos logs. As saídas do comando também podem ser compartilhadas com o Aruba TAC para fins de solução de problemas.

Se tudo estiver funcionando corretamente, você poderá ver uma nova entrada no painel do Umbrella em Implantações > Dispositivos de rede, onde você poderá procurar um cluster de AP instantâneo por seu nome ou excluir uma entrada existente se desejar gerar uma nova ID de dispositivo.



4404011658516

Interceptar consultas DNS

Após confirmar que um cluster foi adicionado com êxito ao painel do Umbrella como um dispositivo de rede, você pode configurar o cluster para começar a interceptar consultas DNS enviadas de clientes sem fio (que estão conectados a APs no cluster). Uma vez definido, independentemente de quais endereços IP do servidor DNS são configurados nas placas de rede dos clientes sem fio, as consultas DNS dos clientes podem ser interceptadas pelo cluster e encaminhadas aos resolvedores anycast da Umbrella em 208.67.220.220 e 208.67.222.222.

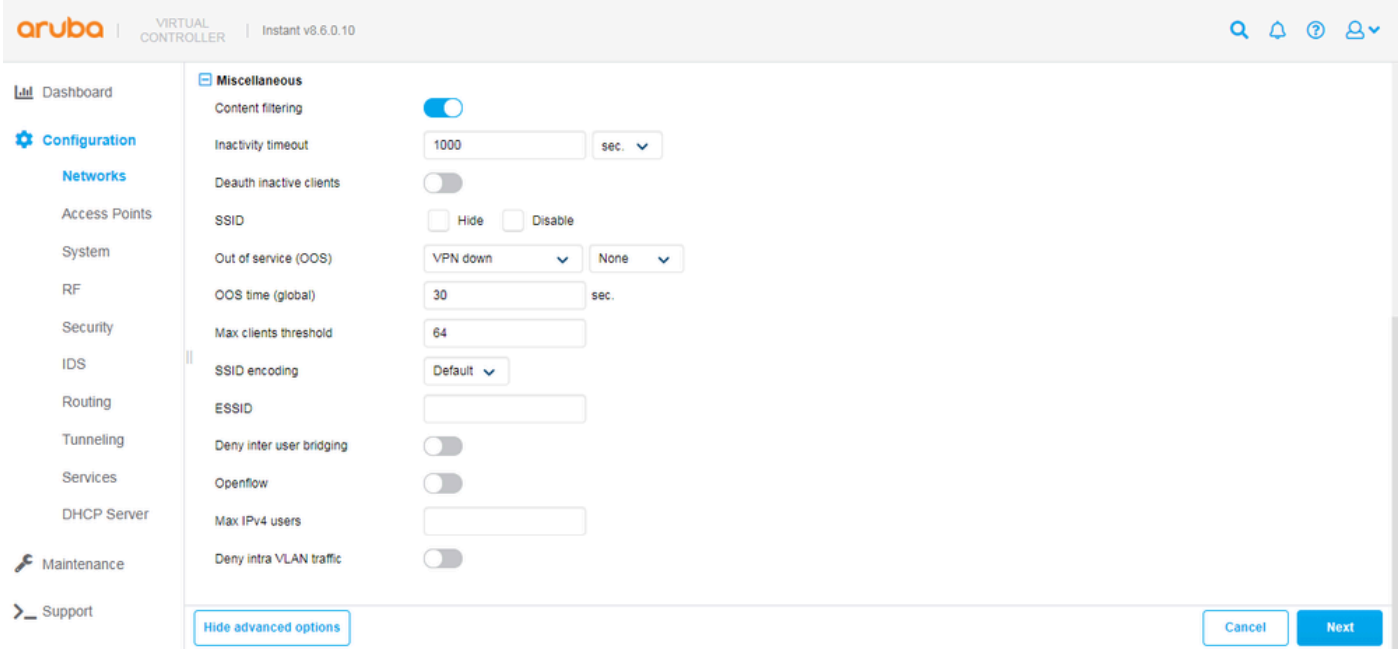
Para interceptar consultas DNS:

1. Navegue até o controlador virtual de um cluster em Configuration > Networks.

2. Selecione uma rede sem fio.

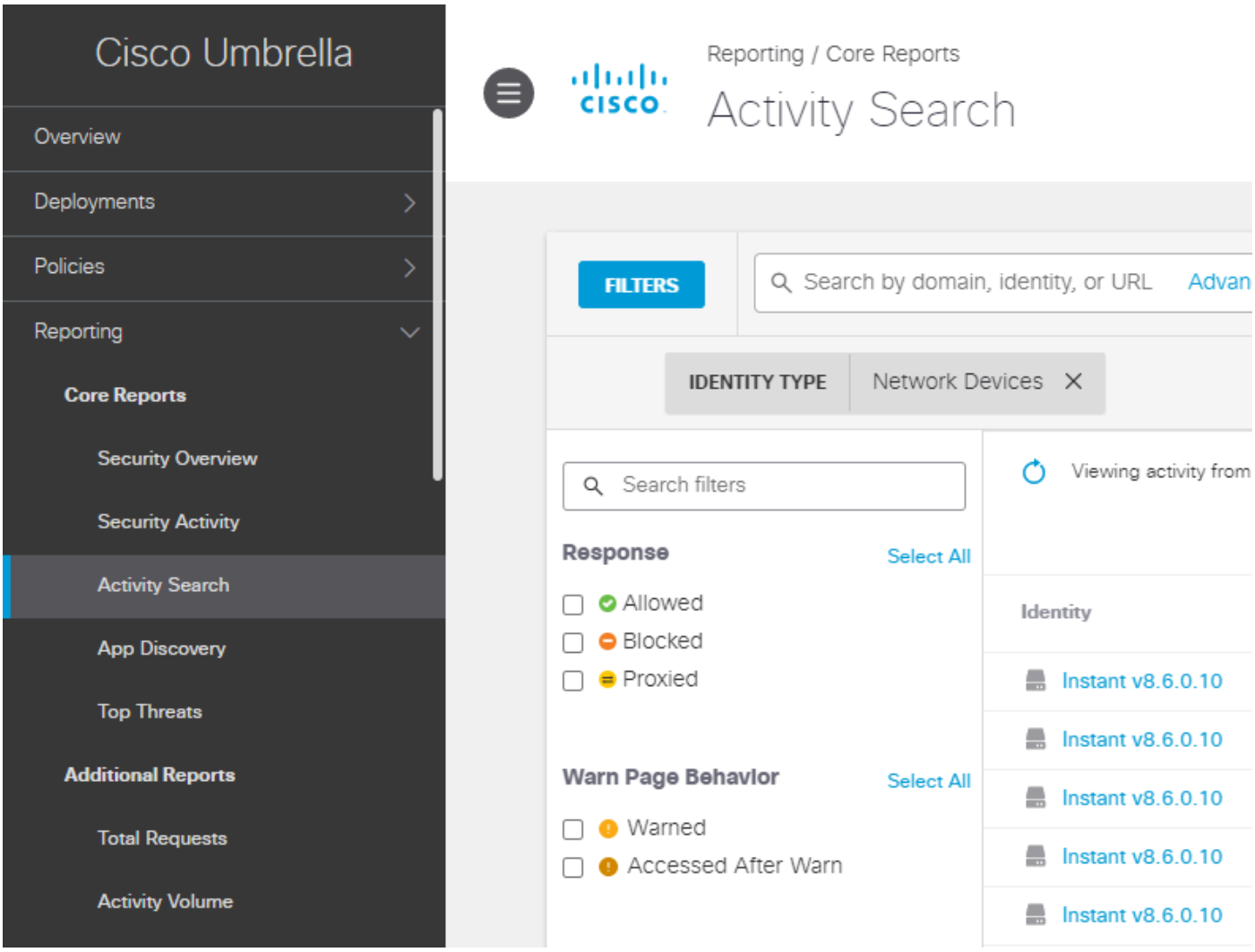
3. Edite a rede, selecione Mostrar opções avançadas e role até a seção Diversos.

4. Ative a opção Filtragem de conteúdo e continue selecionando Próximo até poder selecionar o botão Finalizar para salvar a alteração.



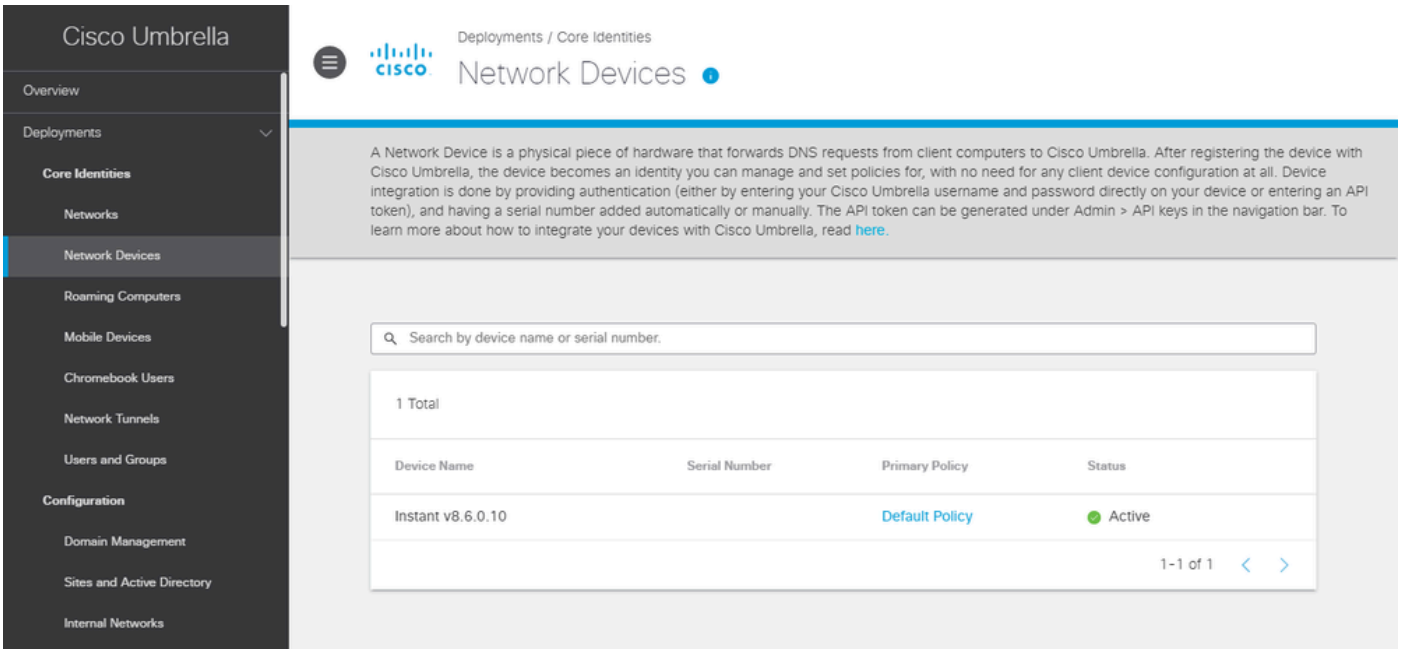
4404011668500

Depois que a opção estiver ativada, você pode começar a ver as consultas DNS no painel Umbrella em Relatórios > Pesquisa de atividade.A identidade das consultas pode ser mapeada para um nome de dispositivo de rede, que geralmente é o nome do sistema configurado em um controlador virtual de cluster AP. Observe que pode levar algum tempo (cerca de 15 minutos) para que as consultas sejam processadas e exibidas na GUI do painel.



4404011721620

No painel Umbrella em Deployments > Network Devices, pode levar até 24 horas para um dispositivo mudar para um status ativo/online. O status de um dispositivo de rede simplesmente indica se as consultas DNS foram interceptadas pelo dispositivo e encaminhadas para o Umbrella nas 24 horas anteriores e não influencia como um dispositivo se comunica com o Umbrella. Um status off-line/inativo pode simplesmente significar que nenhum cliente sem fio foi conectado a um cluster de AP nas últimas 24 horas e não pode impedir o cluster de utilizar o serviço Umbrella.

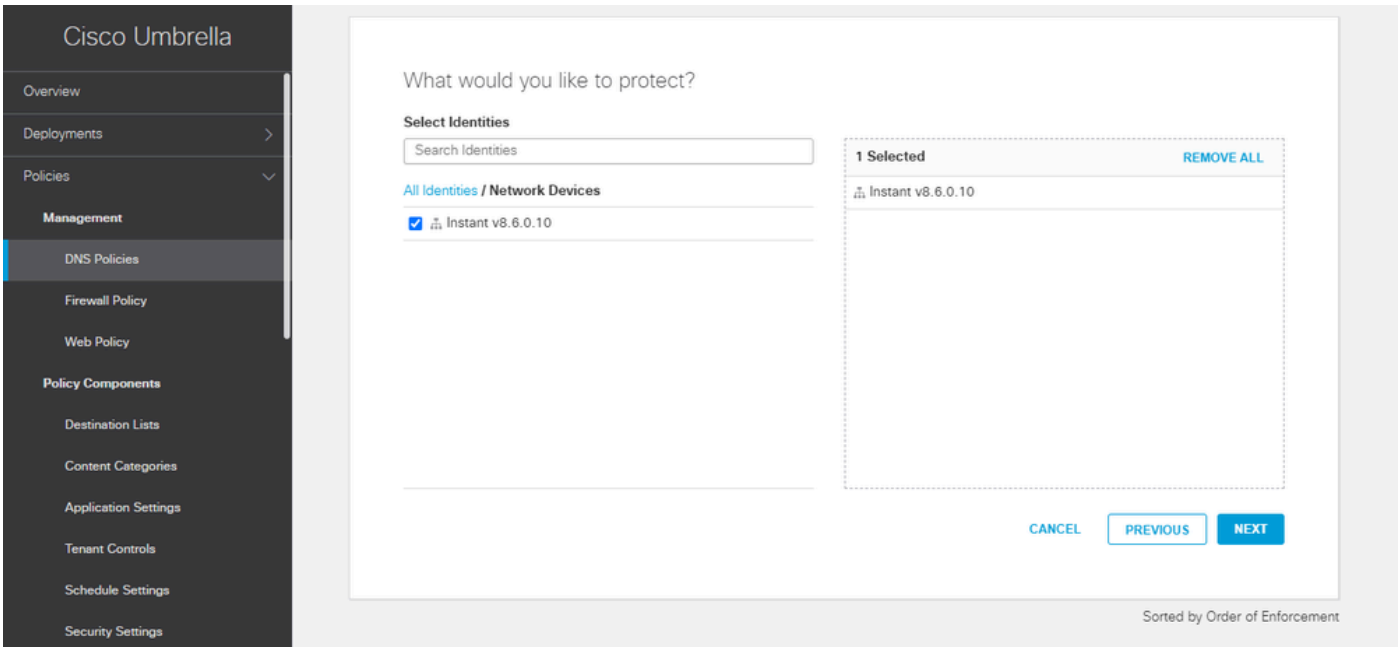


4404011756308

Aplicar Política de DNS

No Umbrella, a "política padrão" inclui automaticamente todas as identidades (como dispositivos de rede) adicionadas a um painel. Não é necessário criar políticas de DNS adicionais se todos os clusters de AP em sua implantação puderem estar sujeitos à mesma política. Se esse for o caso para você, vá para a próxima seção.

Como alternativa, se desejar aplicar uma política personalizada a um dispositivo de rede específico, você precisará adicionar uma nova política no painel do Umbrella em Policies > All Policies (DNS Policies), e selecionar o dispositivo de rede na política.



4404011773588

Quando há mais de uma política na página Políticas de DNS (Todas as Políticas), as políticas são

avaliadas de cima para baixo com base na primeira correspondência. Para obter mais informações, consulte a documentação de precedência de política e as melhores práticas para definir a documentação de políticas.

DNS interno

Em um ambiente onde existem servidores DNS internos e você deseja encaminhar consultas DNS para determinados domínios (internos) para os servidores DNS internos, você pode usar o recurso Domínios corporativos no Instant.

As consultas DNS podem continuar a ser interceptadas pelo cluster AP depois que o recurso é habilitado, exceto pelo fato de que as consultas para os domínios especificados não podem mais ser encaminhadas para o Umbrella. Em vez disso, eles podem ser encaminhados para os endereços IP do servidor DNS configurados originalmente nas NICs dos clientes sem fio (como via DHCP). O recurso é semelhante à funcionalidade Internal Domains disponível nos métodos de implantação Umbrella padrão (com dispositivos virtuais), onde a integração Aruba Instant não é usada.

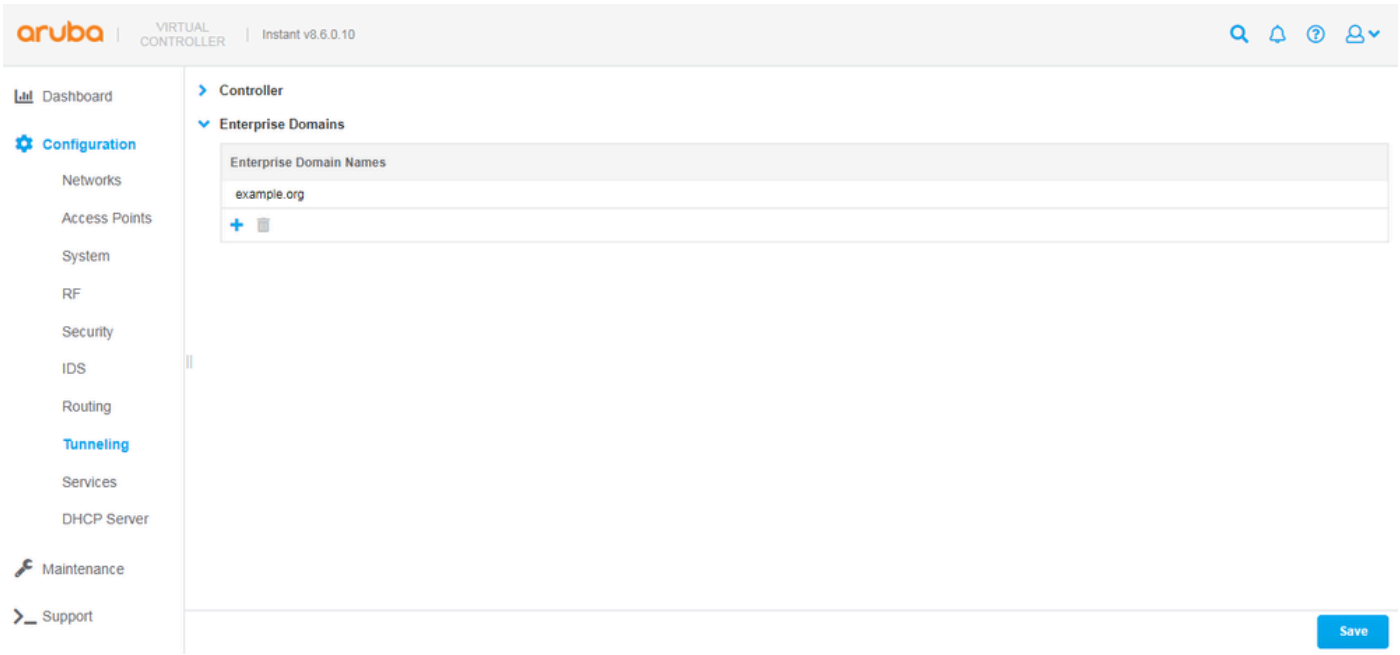
Para configurar o recurso em um controlador virtual instantâneo:

1. Navegue até Configuration > Tunneling > Enterprise Domains.

2. Adicione ou remova domínios da lista Nomes de Domínio da Empresa.

3. Selecione Salvar.

Há um curinga implícito para qualquer domínio adicionado à lista, portanto example.org implica *.example.org.



4404238114452

Verificação

Se você implantou o Umbrella em sua WLAN usando os métodos padrão referenciados na seção "Visão geral da implantação" deste guia, ou a integração descrita na seção "Integração instantânea da Aruba", é possível verificar se os clientes sem fio estão usando o DNS do Umbrella navegando até https://welcome.umbrella.com/ de um dos clientes. Em seguida, você verá uma marca de seleção verde semelhante à captura de tela exibida na documentação do Umbrella.

4404011960212

Como alternativa, você pode verificar isso executando esse comando no prompt de comando de um cliente sem fio.

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

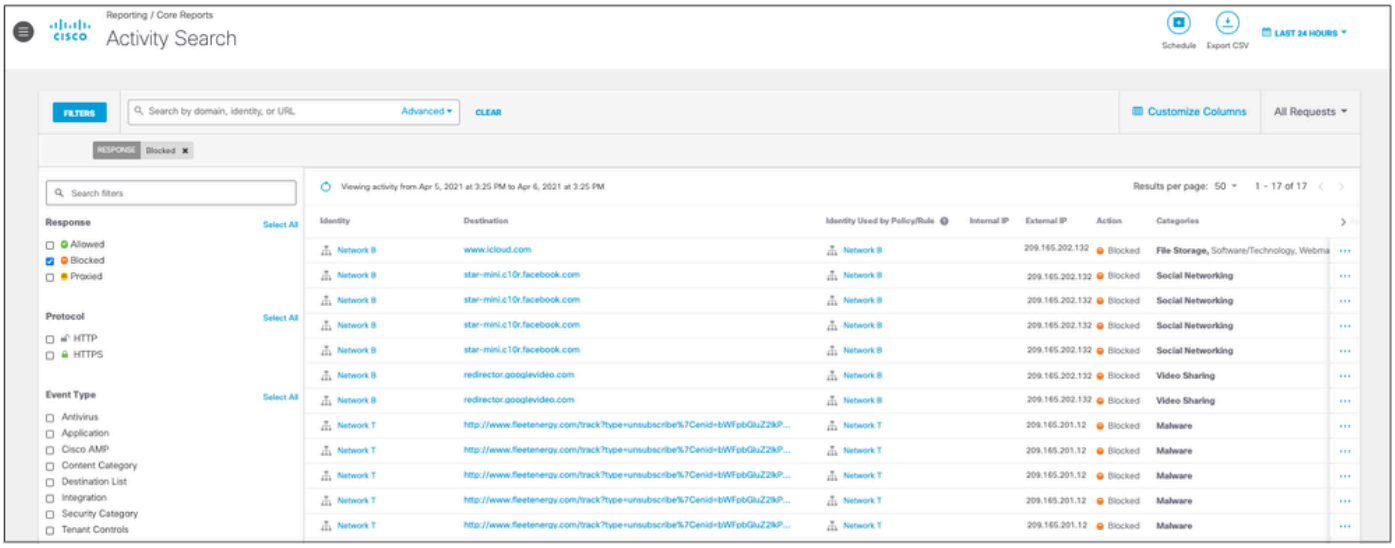
Você pode ver uma saída com um número de linhas de texto, semelhante a esta captura de tela:

```
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
debug.opendns.com       text = "appliance id
debug.opendns.com       text = "host id
debug.opendns.com       text = "user id
debug.opendns.com       text = "remoteip
debug.opendns.com       text = "flags
debug.opendns.com       text = "id
debug.opendns.com       text = "source
debug.opendns.com       text = "fw: flags
debug.opendns.com       text = "fw: id
debug.opendns.com       text = "fw: source

Authoritative answers can be found from:

anthony@ubuntu:~/Desktop$
```

4404011980436

Na saída do comando, você pode ver a ID da organização do painel do Umbrella na linha "orgid" ou "id da organização" e, se você usar a integração instantânea, poderá ver a linha extra "device" que contém uma ID de dispositivo.

Para revisar as consultas DNS no painel Umbrella, navegue para Relatórios > Pesquisa de atividade. Observe que pode levar algum tempo (cerca de 15 minutos) para que as consultas sejam exibidas na GUI do painel. As instruções sobre como usar a Pesquisa de atividades estão disponíveis em na documentação do Umbrella.



4404019393044

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.