为Aruba WLAN管理员部署Umbrella DNS

目录

简介

本文档介绍如何为Aruba WLAN管理员部署Umbrella DNS服务。

先决条件

要求

本文档没有任何特定的要求。

使用的组件

本文档中的信息基于Cisco Umbrella。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

概述

Aruba Networks针对不同的细分市场和部署方案提供以下三个无线局域网(WLAN)产品线和操作系统：

- ArubaOS：适用于大型组织和高密度部署
- Aruba Instant / InstantOS：适用于中小型企业和分布式企业

- Aruba Instant开启： 适用于家庭和小型办公室用户

本文为Aruba WLAN管理员采用和部署Umbrella DNS服务提供了指导原则。

部署方法

部署方法取决于您的Aruba操作系统以及您计划如何使用Umbrella。

如果您运行上述三种Aruba操作系统中的任何一种，则可以通过Umbrella用户指南开始部署Umbrella DNS。视频教程也可用。

如果运行Aruba Instant，您还可以选择使用InstantOS中提供的Umbrella网络设备集成。但是，请注意，如果选择此选项，则在Umbrella报告(如Activity Search报告)中无法看到WLAN上无线客户端的内部/私有IP地址。来自客户端的DNS查询映射到Umbrella中的即时AP集群的网络设备身份，有关各个客户端的信息不可用。从Umbrella云的角度来看，DNS查询似乎来自即时AP集群，而不是Wi-Fi客户端。

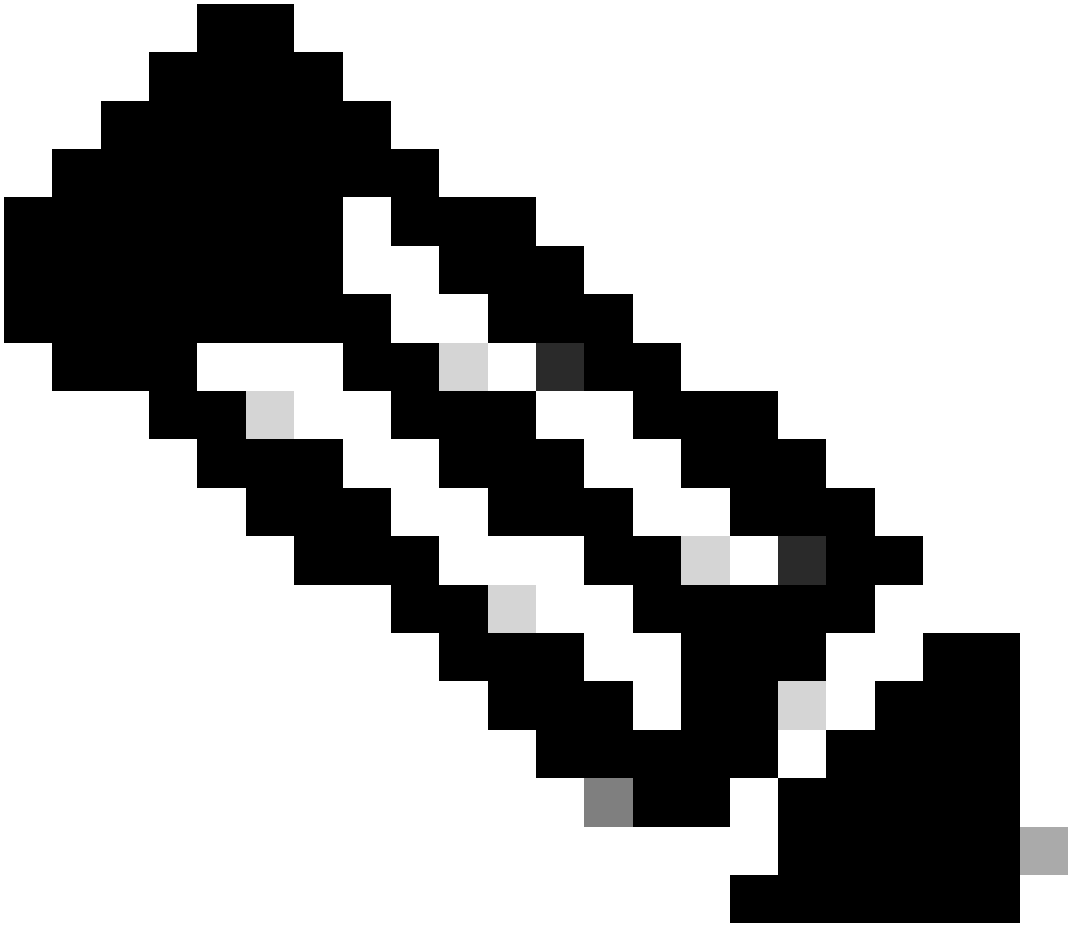
因此，如果您需要跟踪单个客户端的DNS查询或为WLAN上的单个客户端定制DNS策略，您可以通过Umbrella DNS用户指南中介绍的标准方法部署Umbrella（无需使用Aruba Instant网络设备集成），并考虑将Umbrella虚拟设备纳入部署计划。

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

Aruba即时集成

Aruba Instant的Umbrella(OpenDNS)网络设备集成在如下环境中会很有用：连接到即时AP集群的所有Wi-Fi客户端都受制于单一的Umbrella DNS策略，并且无需在Umbrella报告中查看单个客户端的DNS查询。本节介绍如何设置集成。



注意：该集成使用Umbrella网络设备API的旧版本。旧版不要求客户从其Umbrella控制面板生成API令牌，但新版需要。

Umbrella传统API在2023-09-01达到寿命终止状态，此后不再为集成提供日期支持。如果您在2023-09-01之后遇到任何集成问题，请完成部署指南中的“入门”部分，以在不使用集成的情况下部署Umbrella。

要使用此集成，需要满足以下要求：

- AP需要运行InstantOS版本8.10.0.1或更高版本（截至2022年5月）。
- 用于集成的Umbrella控制面板帐户需要具有Full Admin角色。
- 帐户的电子邮件地址不能与多个Umbrella控制面板关联。如果您不确定该电子邮件地址是否只与单个控制面板关联，您可以联系Cisco Umbrella支持以进行验证。
- 无法为帐户启用单点登录(SSO)和双因素身份验证(2FA)。
- 如果AP和Internet之间存在网络安全设备（如防火墙），则设备需要允许到208.67.220.220、208.67.222.222、67.215.92.210和146.112.255.152/29(.152 ~ .159)的未过滤和未检查连接。

配置

在较高层面上，启用集成有四个配置步骤：

1.设置AP集群的名称

2.输入帐户凭证

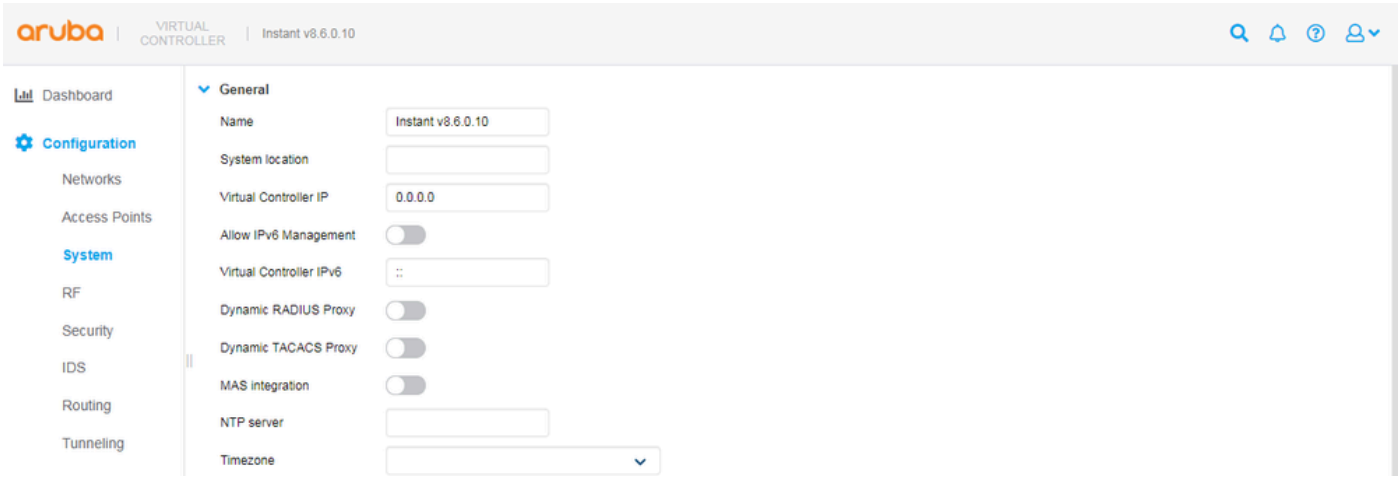
3.拦截DNS查询

4.应用DNS策略

设置AP集群的名称

当即时集群首次成功将自身注册到Umbrella控制面板时，网络设备条目将添加到部署>网络设备下的Umbrella控制面板。新条目的设备名称来自在集群的虚拟控制器上配置的系统名称。

要在即时虚拟控制器上设置系统名称，请导航到配置>系统。



4404011628308

请注意，在初始注册期间，仅复制一次名称值。如果系统/设备名称随后在Instant或Umbrella端发生更改，则必须手动更新另一端的名称。

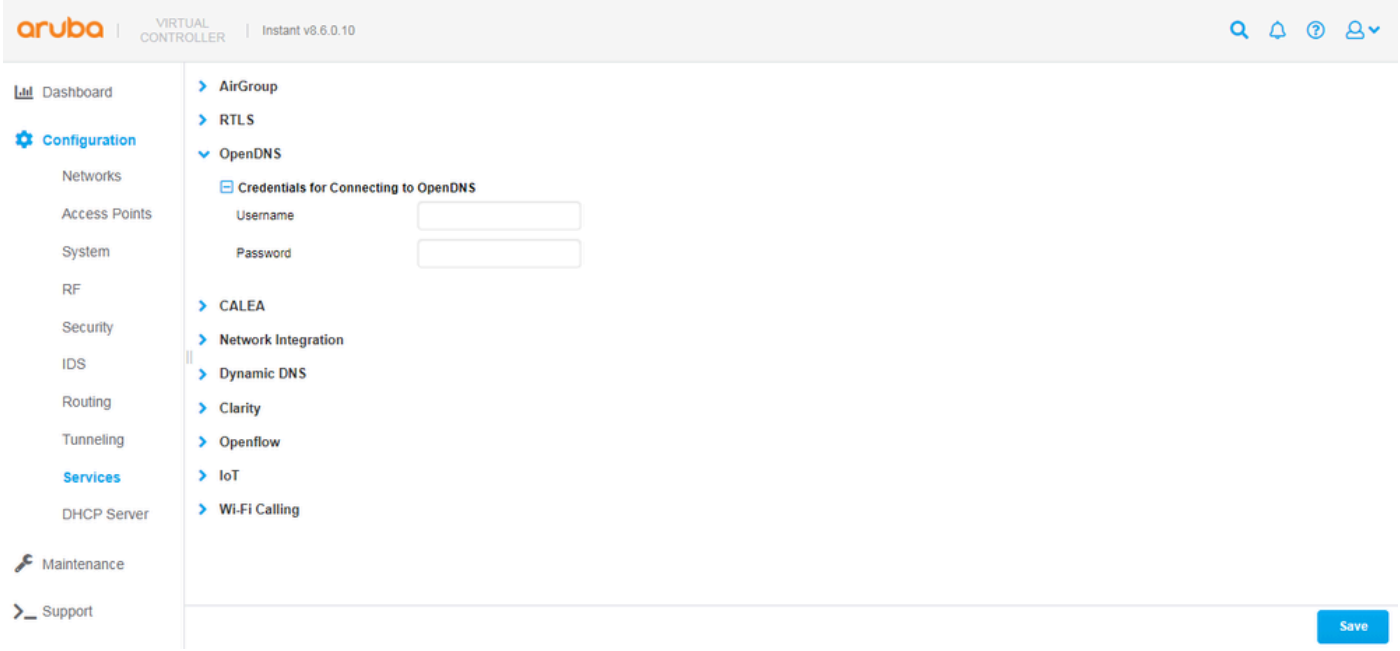
输入帐户凭证

如果满足先决条件部分列出的要求，您可以将即时集群作为网络设备添加到Umbrella控制面板。要从集群的虚拟控制器执行此操作：

1.导航到配置>服务> OpenDNS。

2.输入Umbrella帐户的登录凭证。

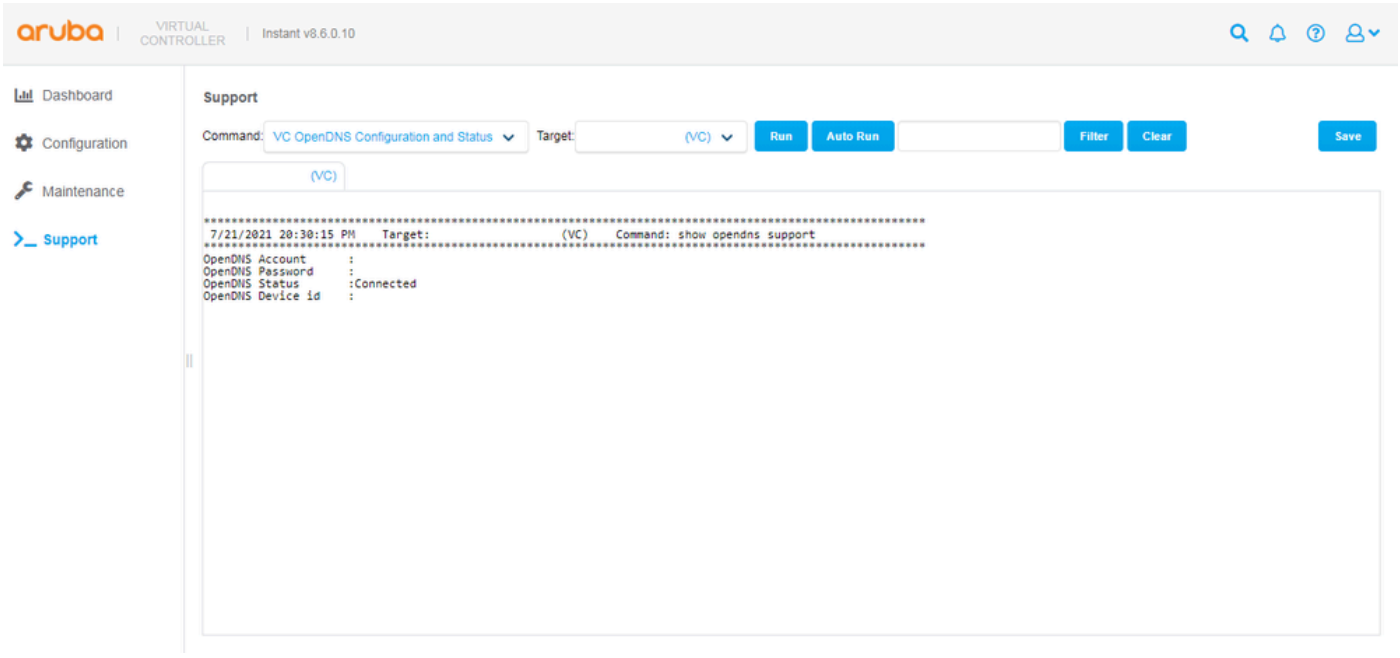
3.选择保存。



4404019266196

如果虚拟控制器(VC)成功连接到Umbrella，则导航到Support并运行“VC OpenDNS Configuration and Status”(`show opendns support`)命令时，您可以看到Connected状态。

您还可以看到设备ID，它由Umbrella在创建新网络设备并保存到即时VC配置中时生成。后一部分很重要。由于每个即时集群都需要具有唯一的Umbrella网络设备ID，因此不能将设备ID从一个集群的配置复制到另一个集群。有效的设备ID通常有16位数字。

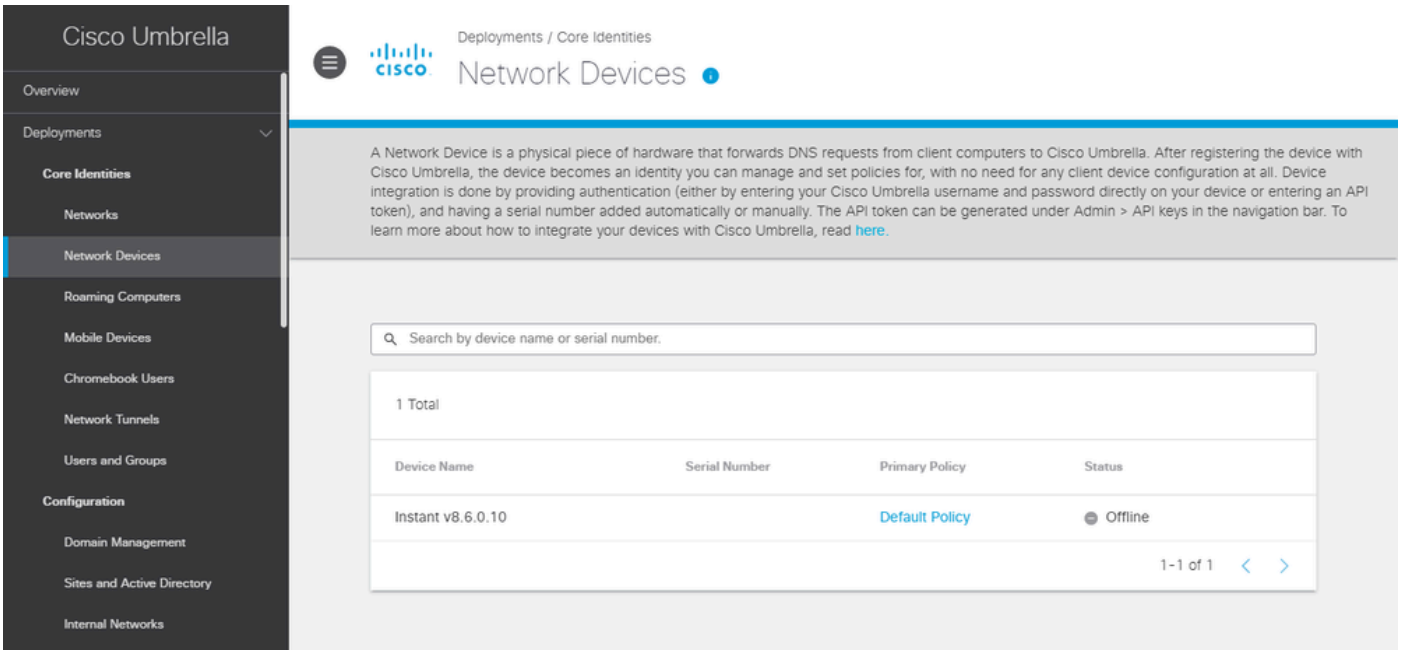


4404019268116

如果命令输出显示Not connected状态，您可以尝试通过运行“AP技术支持转储”(`show tech-support`)和“AP技术支持转储补充”(`show tech-support supplemental`)命令，然后在日志中搜索“opendns”来找出原因。也可与Aruba TAC共享命令输出以进行故障排除。

如果一切正常，您可以在Umbrella控制面板中的部署>网络设备下看到一个新条目，您可以在该控制

面板中按名称搜索即时AP集群，或者删除现有条目（如果您希望生成新的设备ID）。



4404011658516

拦截DNS查询

确认集群已作为网络设备成功添加到Umbrella控制面板后，可以将集群设置为开始拦截从无线客户端（连接到集群中的AP）发送的DNS查询。 设置后，无论无线客户端的网卡上配置了哪些DNS服务器IP地址，客户端的DNS查询都会被集群截取，并转发到Umbrella的任播解析器208.67.220.220和208.67.222.222。

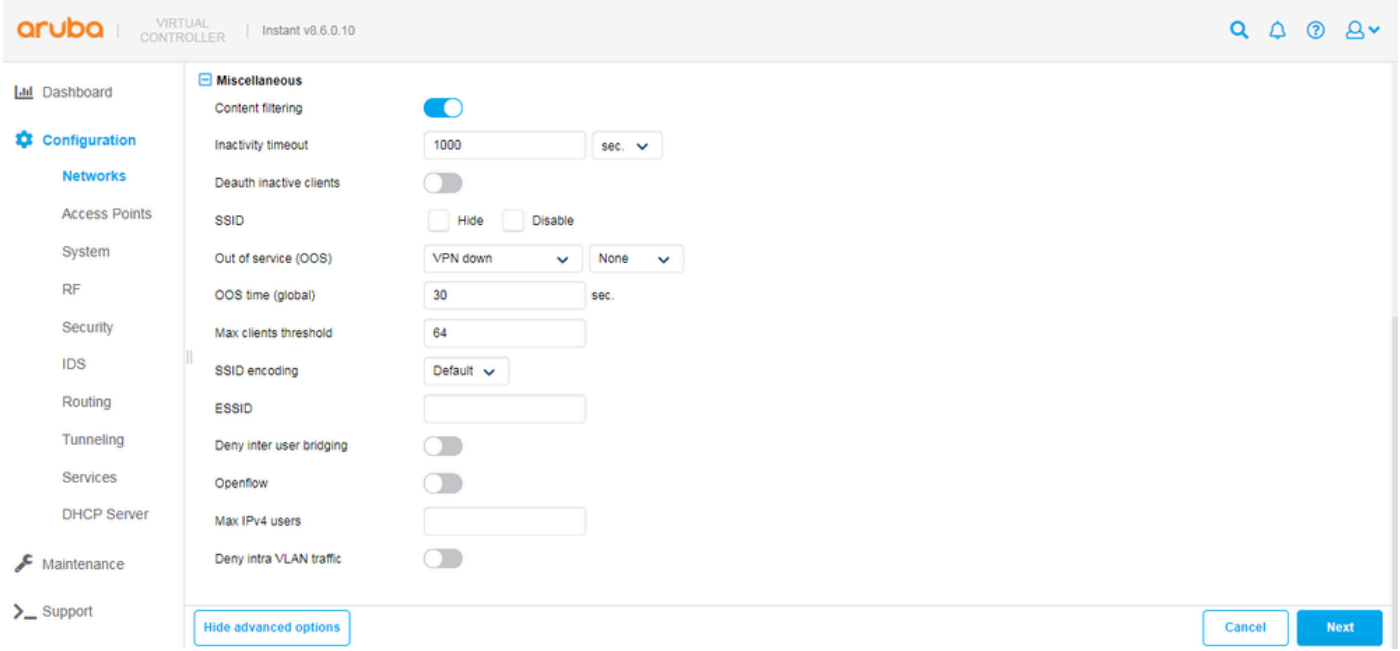
要拦截DNS查询：

1.在Configuration > Networks下导航到集群的虚拟控制器。

2.选择无线网络。

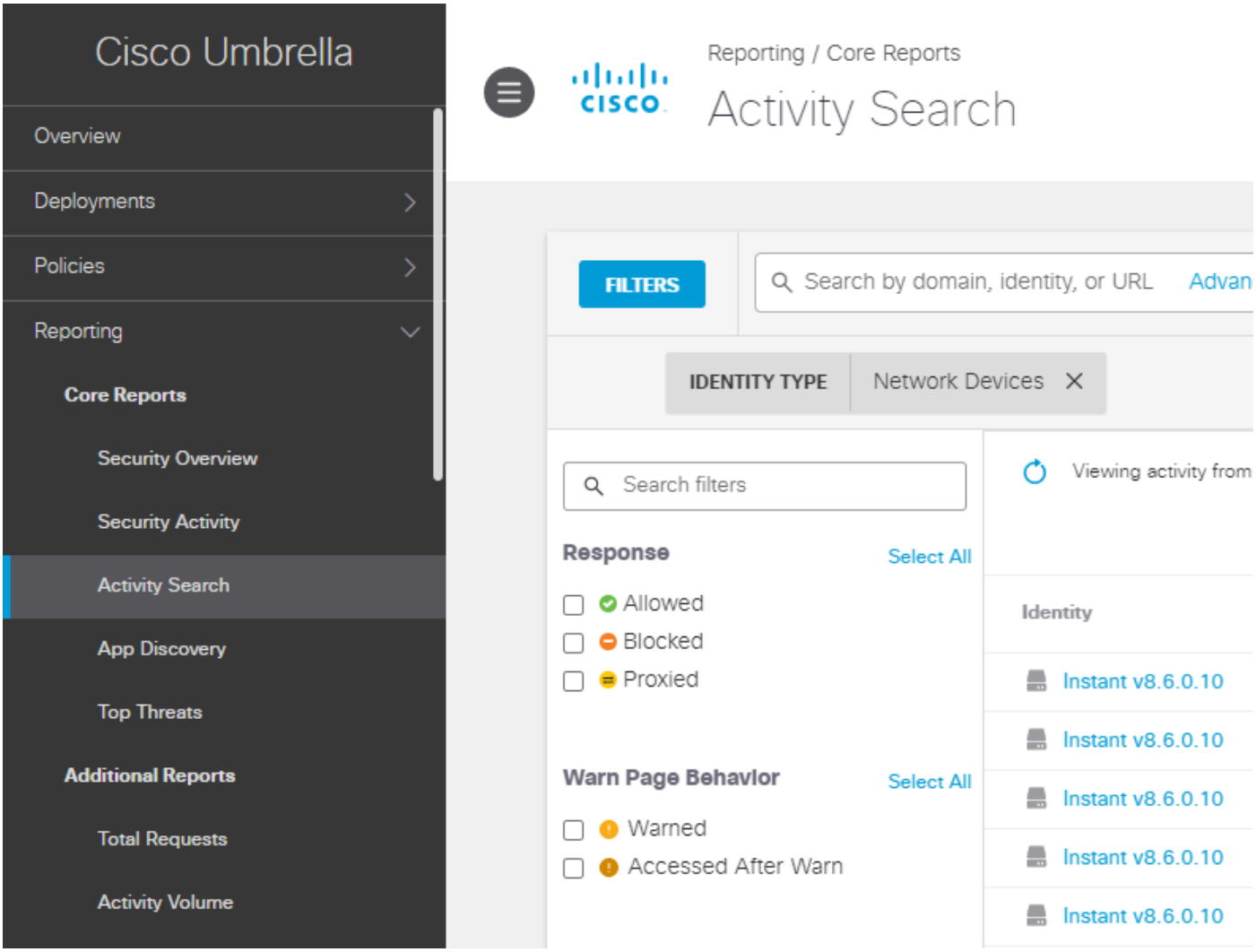
3.编辑网络，选择显示高级选项，然后滚动到其他部分。

4.启用内容过滤选项，并继续选择下一步，直到可以选择完成按钮以保存更改。



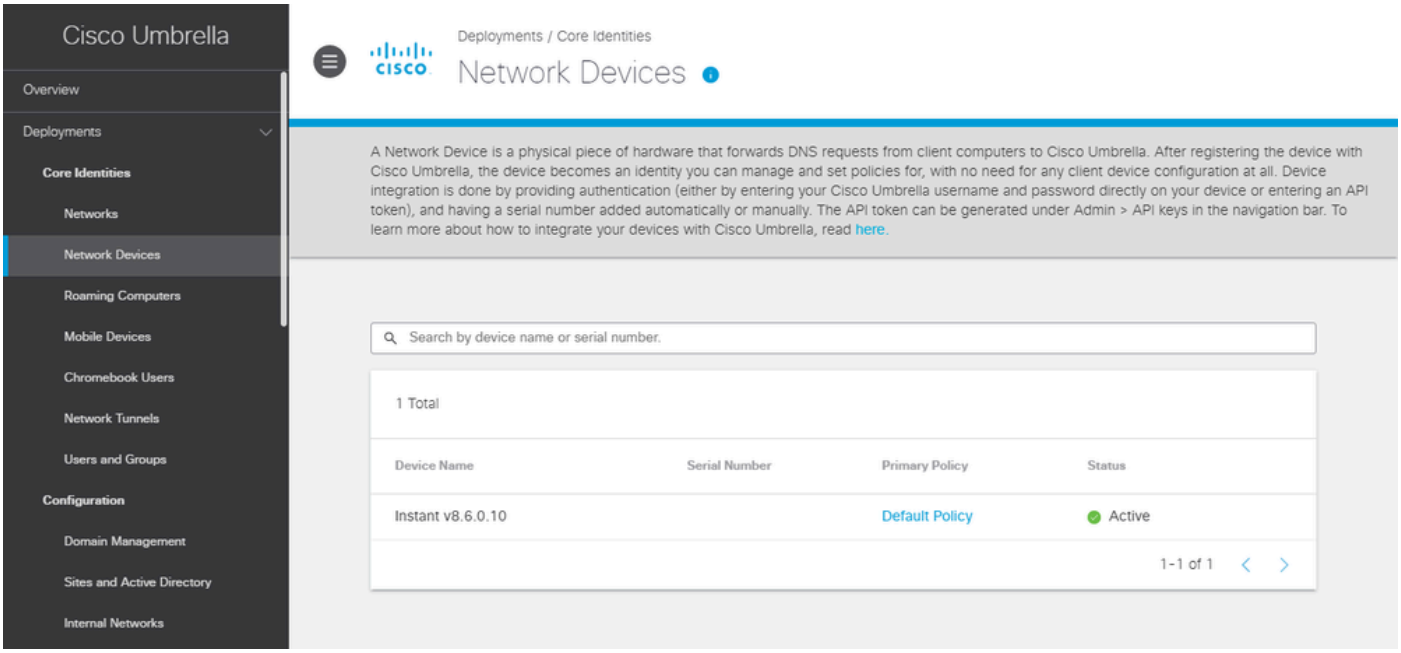
4404011668500

启用该选项后，您可以在Umbrella控制面板中的Reporting > Activity Search下查看DNS查询。查询的标识可以映射到网络设备名称，通常是AP集群的虚拟控制器上配置的系统名称。请注意，在控制面板GUI中处理和显示查询可能需要一些时间（大约15分钟）。



4404011721620

在部署>网络设备下的Umbrella控制面板中，设备最多可能需要24小时才能更改为活动/联机状态。网络设备的状态仅表示DNS查询是否在之前的24小时内被设备拦截并转发到Umbrella，而不影响设备与Umbrella的通信方式。脱机/非活动状态可能仅仅意味着在过去24小时内没有无线客户端连接到AP集群，并且无法阻止集群使用Umbrella服务。

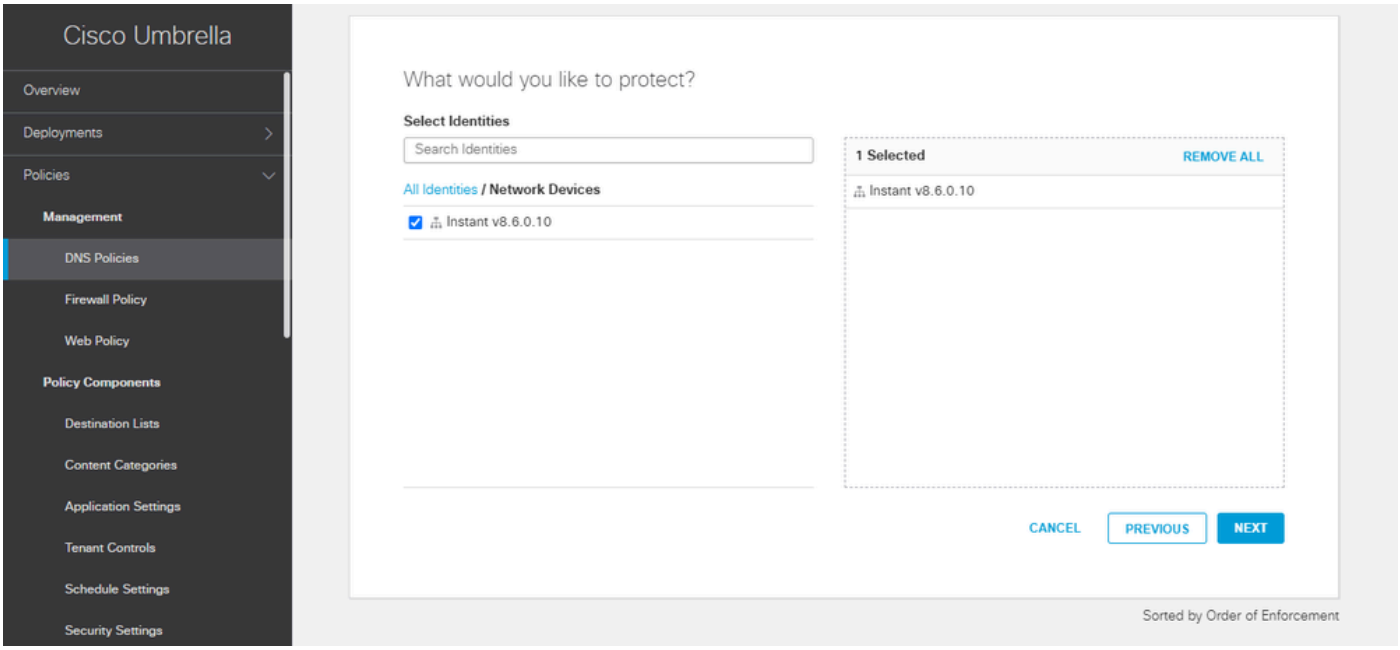


4404011756308

应用DNS策略

在Umbrella中，“默认策略”自动包括添加到控制面板的所有身份（如网络设备）。如果部署中的所有AP集群都受同一策略约束，则无需创建其他DNS策略。如果您是这种情况，请跳至下一节。

或者，如果要将自定义策略应用于特定网络设备，则需要在Policies > All Policies(DNS Policies) 下的Umbrella控制面板中添加新策略，然后在策略中选择网络设备。



4404011773588

当DNS Policies(All Policies)页面上存在多个策略时，策略会按照从上到下的顺序进行第一次匹配评估。有关详细信息，请参阅策略优先文档和定义策略文档的最佳实践。

内部DNS

在存在内部DNS服务器，并且要将特定（内部）域的DNS查询转发到内部DNS服务器的环境中，您可以在即时中使用Enterprise Domains功能。

启用此功能后，AP集群可以继续拦截DNS查询，但指定域的查询无法再转发到Umbrella。相反，它们可以转发到最初在无线客户端的NIC上配置的DNS服务器IP地址（例如通过DHCP）。 此功能类似于标准Umbrella部署方法（使用虚拟设备）中提供的Internal Domains功能，其中不使用Aruba Instant集成。

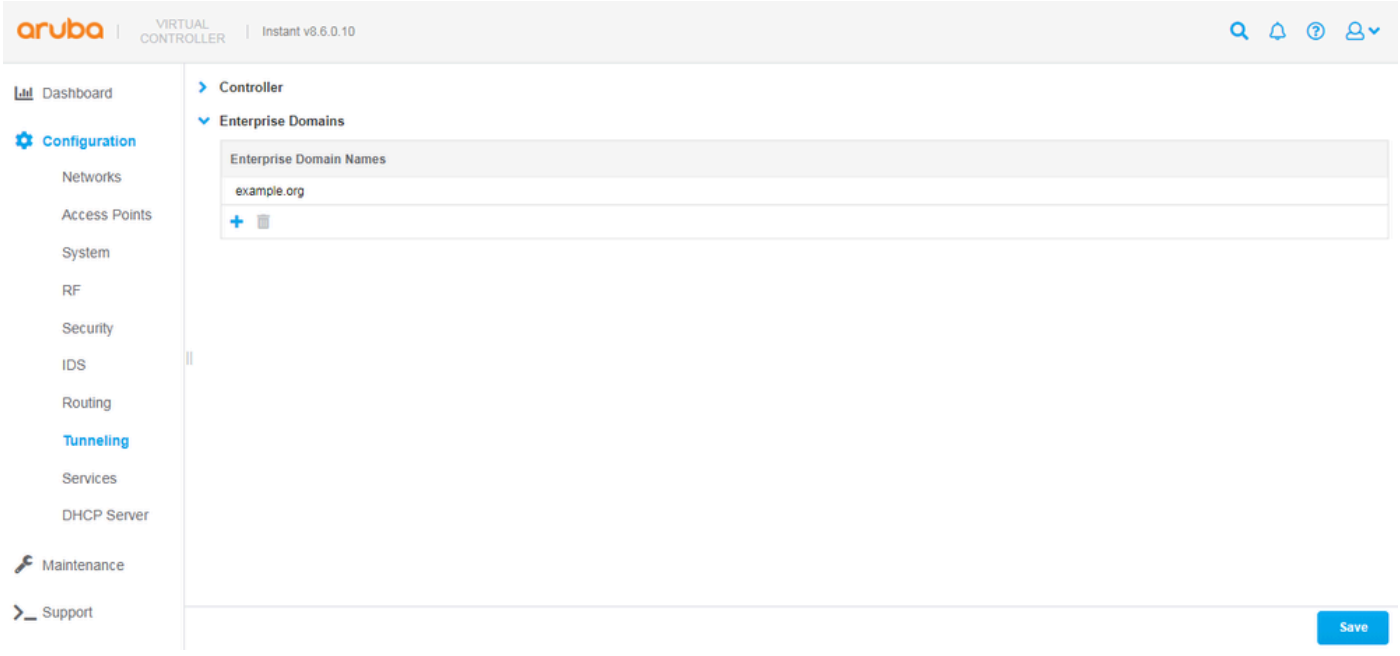
要在即时虚拟控制器上配置功能，请执行以下操作：

1.导航到配置>隧道>企业域。

2.在“企业域名”列表中添加域或从中删除域。

3.选择保存。

对于添加到列表中的任何域，都有一个隐式通配符，因此example.org表示*.example.org。

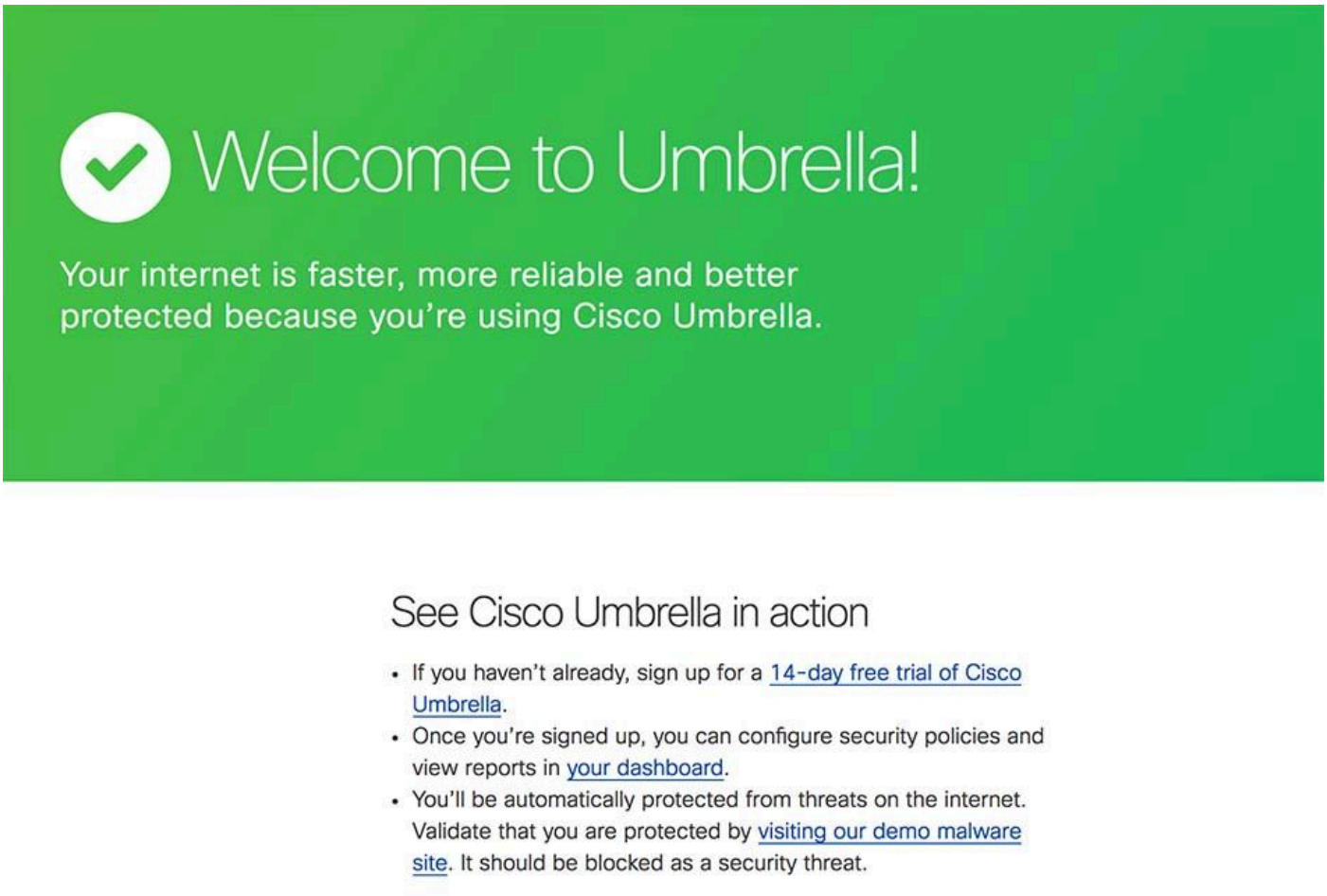


4404238114452

确认

无论您是使用本指南的“部署概述”部分中提到的标准方法在WLAN上部署Umbrella，还是使用“Aruba即时集成”部分中描述的集成，您都可以通过从其中一个客户端浏览到https://welcome.umbrella.com/来验证无线客户端是否正在使用Umbrella DNS。然后，您会看到与

Umbrella文档中显示的屏幕截图类似的绿色勾选。



4404011960212

或者，您可以在无线客户端的命令提示符下运行此命令来验证这一点。

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

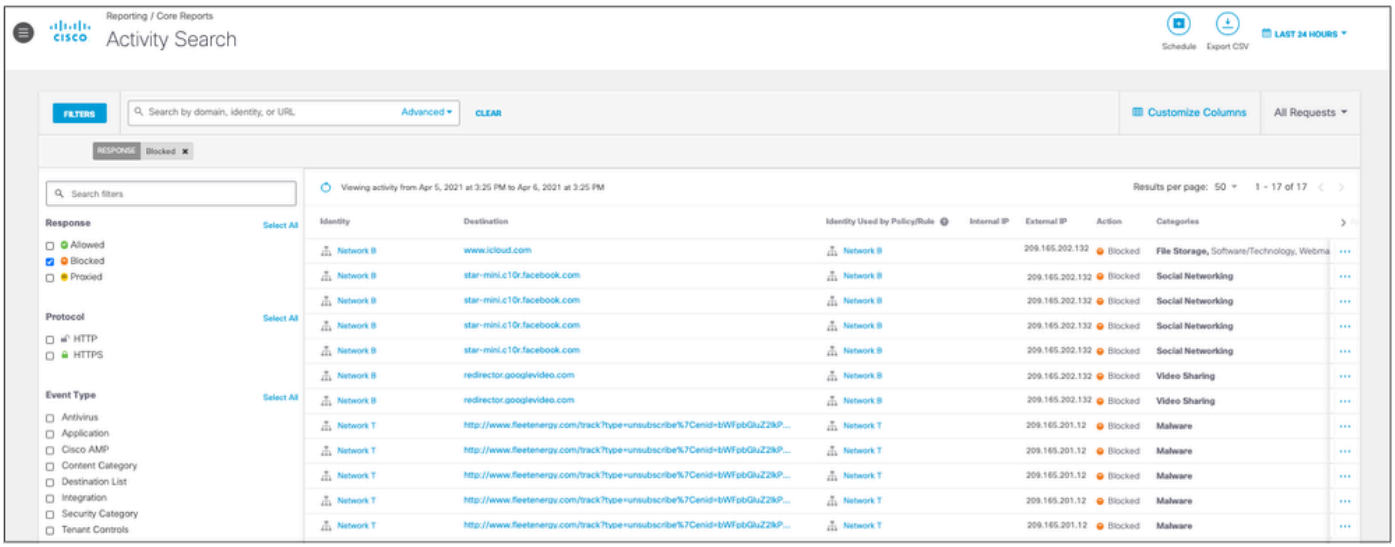
您可以看到包含许多文本行的输出，类似于以下屏幕截图：

```
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

从命令输出中，您可以在“orgid”或“organization id”行中看到Umbrella控制面板的组织ID，如果使用即时集成，则可以看到包含设备ID的额外“设备”行。

要查看Umbrella控制面板中的DNS查询，请导航至报告>活动搜索。请注意，在控制面板GUI中显示查询可能需要一些时间（大约15分钟）。有关如何使用“Activity Search”的说明，请参见Umbrella文档。



4404019393044

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。