# 为Secure Connect用户配置远程访问的SIG策略

## 目录


简介

概述

DNS策略

防火墙策略

Web策略

- Web用户标识

DLP策略

- DLP用户标识


## 简介

本文档介绍如何为Secure Connect用户创建远程访问的SIG策略。

## 概述

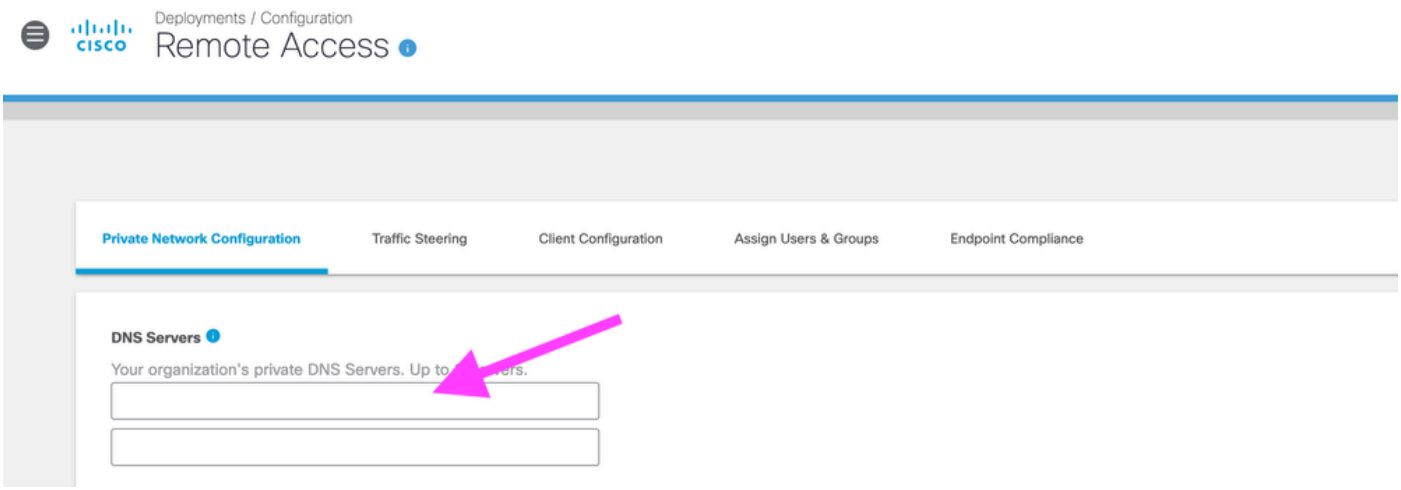
本知识库文章适用于使用Secure Connect软件包的客户，该软件包包含Umbrella中的远程访问(VPNaaS)功能。

管理员可以配置Umbrella防火墙、Web和数据丢失策略以应用于通过AnyConnect连接到远程访问的漫游用户。

## DNS策略

可以向Umbrella解析器(例如208.67.222.222)。但是，这不能在Umbrella控制面板上启用DNS流量的识别、策略或报告。

- 这仅提供DNS解析，因此通常不建议使用。
- 在VPN DNS配置中使用外部DNS解析器可防止解析内部DNS区域。

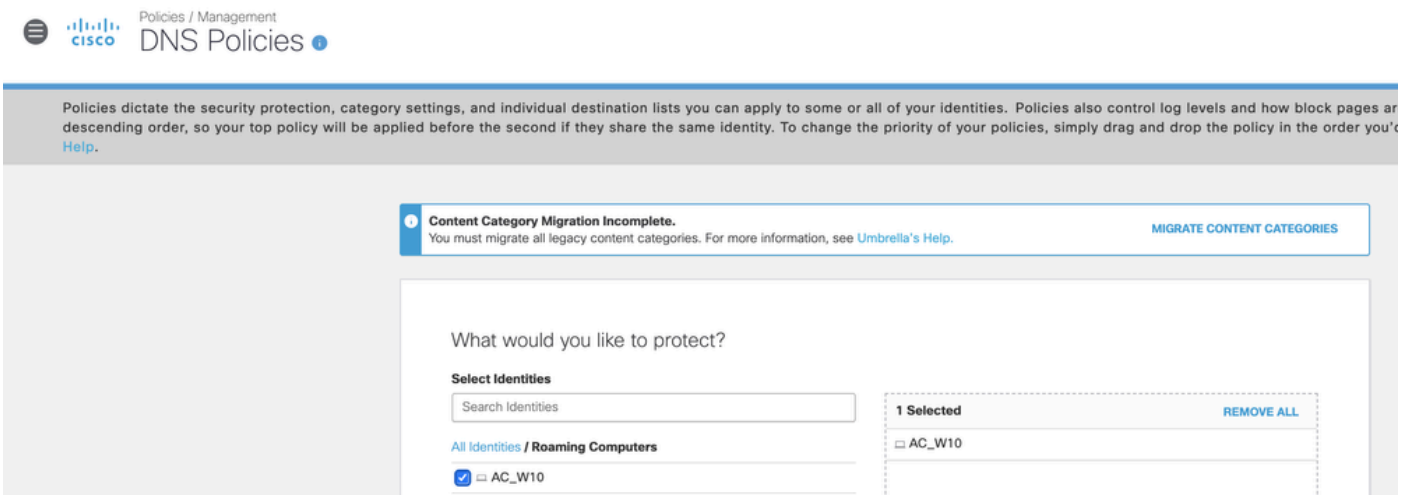



4410210378004

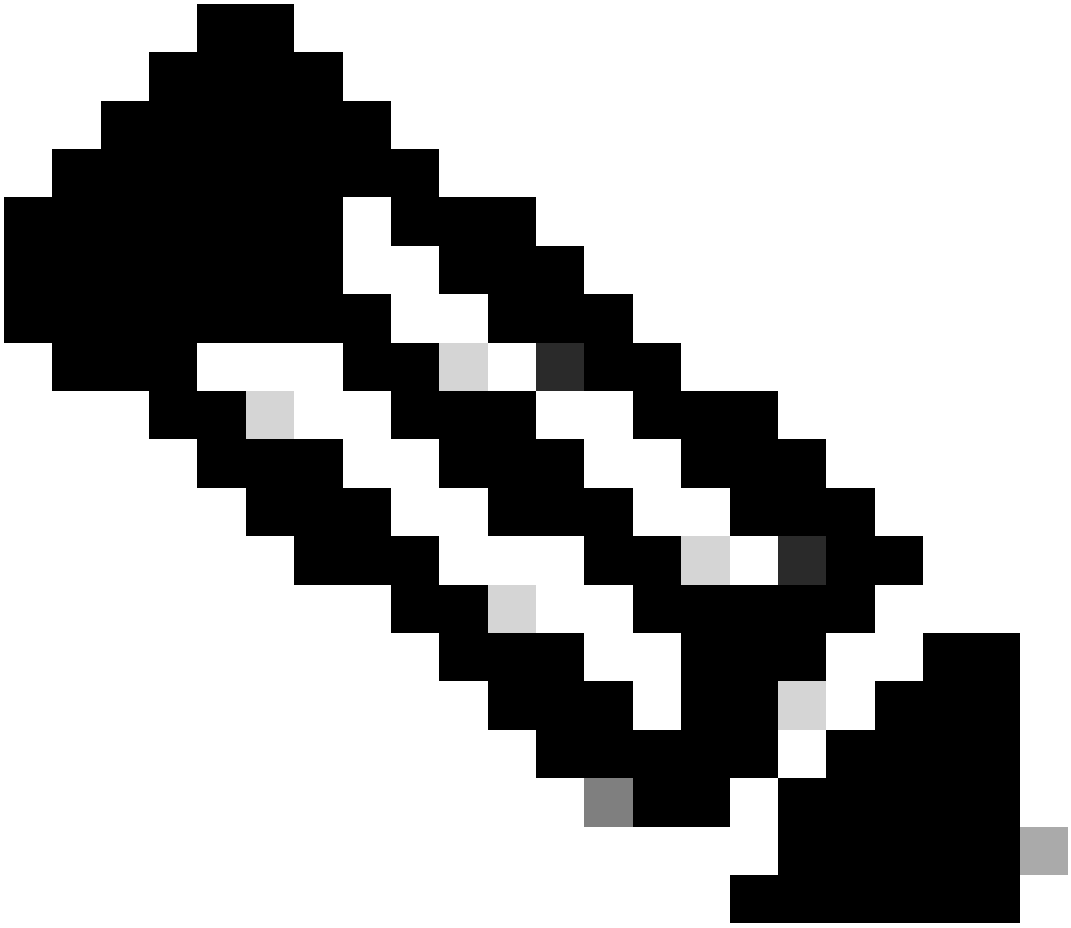
要为DNS查询添加身份、策略和报告，必须考虑以下三种方法之一：

- （推荐）— 部署Umbrella AnyConnect漫游模块（从Deployments > Roaming Computers）。 外部DNS流量直接发送到Umbrella，并应用“漫游计算机”身份。此模块还支持可选的AD用户标识。
- 将流量从本地DNS服务器转发到Umbrella，并使用网络身份识别流量。所有用户都收到相同的策略/身份，并且没有精细的用户报告。
- 在您的内部网络使用Umbrella Virtual Appliance将流量转发到Umbrella。DNS查询可以通过其内部（VPN池IP地址）进行识别。可以添加AD集成 — 需要安装其他内部组件。

此示例显示如何为单个AnyConnect客户端配置DNS策略(Policies > DNS Policies) — 仅当部署了Umbrella AnyConnect漫游模块时，才可能配置DNS策略：




4410210455444



注意：使用Umbrella模块进行AnyConnect时，可以根据您的分割隧道配置，在隧道内部或外部发送DNS流量。

## 防火墙策略

防火墙策略适用于远程访问(AnyConnect)客户端和互联网之间的流量。 根据以下文档在部署>防火墙策略中配置规则： 管理防火墙。

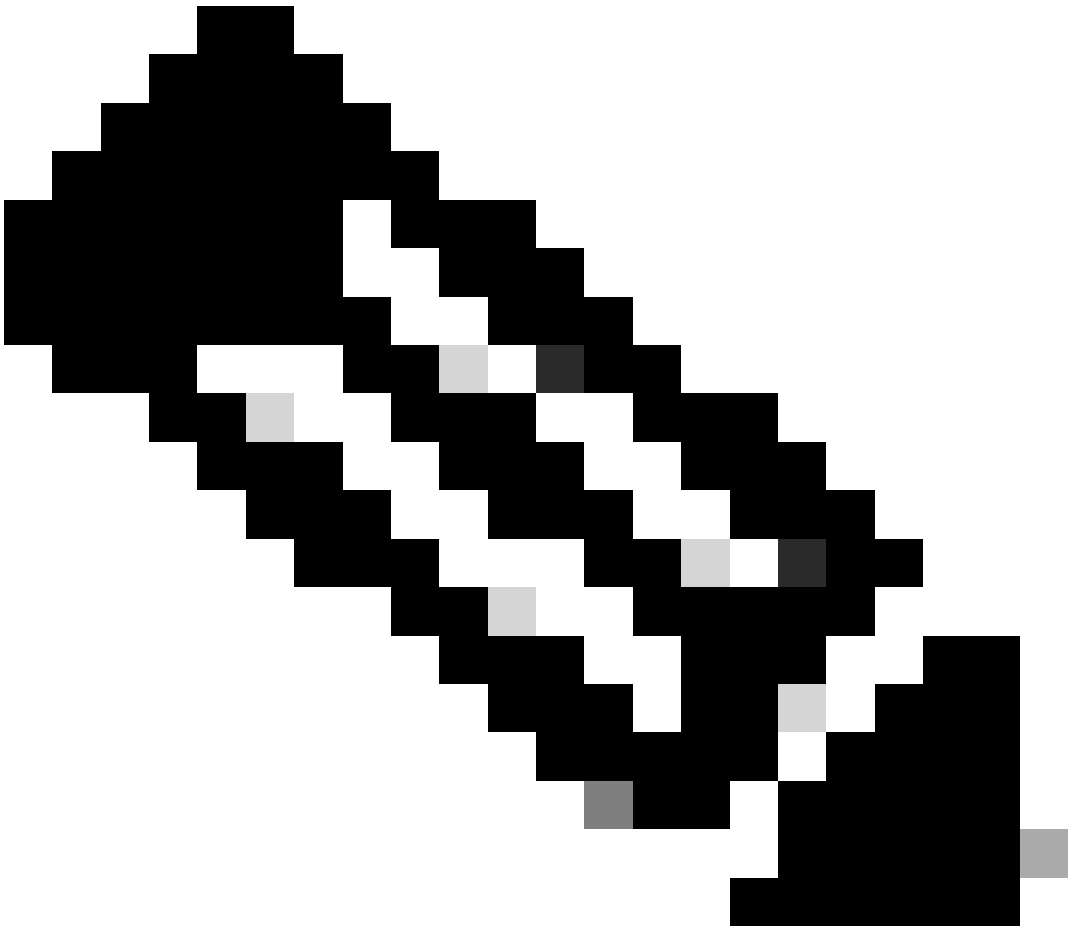
默认防火墙规则适用于远程访问客户端。 如果要为远程访问用户创建特定策略，则可以选择创建新的防火墙策略，然后选择“Remote Access orgid:<ID>”作为源隧道标识。
相同的防火墙策略适用于所有远程访问用户。

- 防火墙策略不用于控制RA客户端和专用/分支机构网络之间的访问。这必须由内部部署防火墙控制。
- 与所有Umbrella防火墙规则一样，这些规则控制远程访问客户端的出站连接。不允许入站连接。
- 远程访问客户端的源IP地址始终从VPN池动态分配。

- 建议不要使用“源IP”为特定计算机创建规则，因为IP是动态重新分配的
- 通过使用“源CIDR”范围，可以创建影响特定远程访问数据中心的用户的规则。 每个数据中心都提供在“Deployments > Remote Access”（部署>远程访问）页面上配置的不同VPN池范围。


4409322341524

---



注意：每个用户标识对于防火墙策略不可用。

---

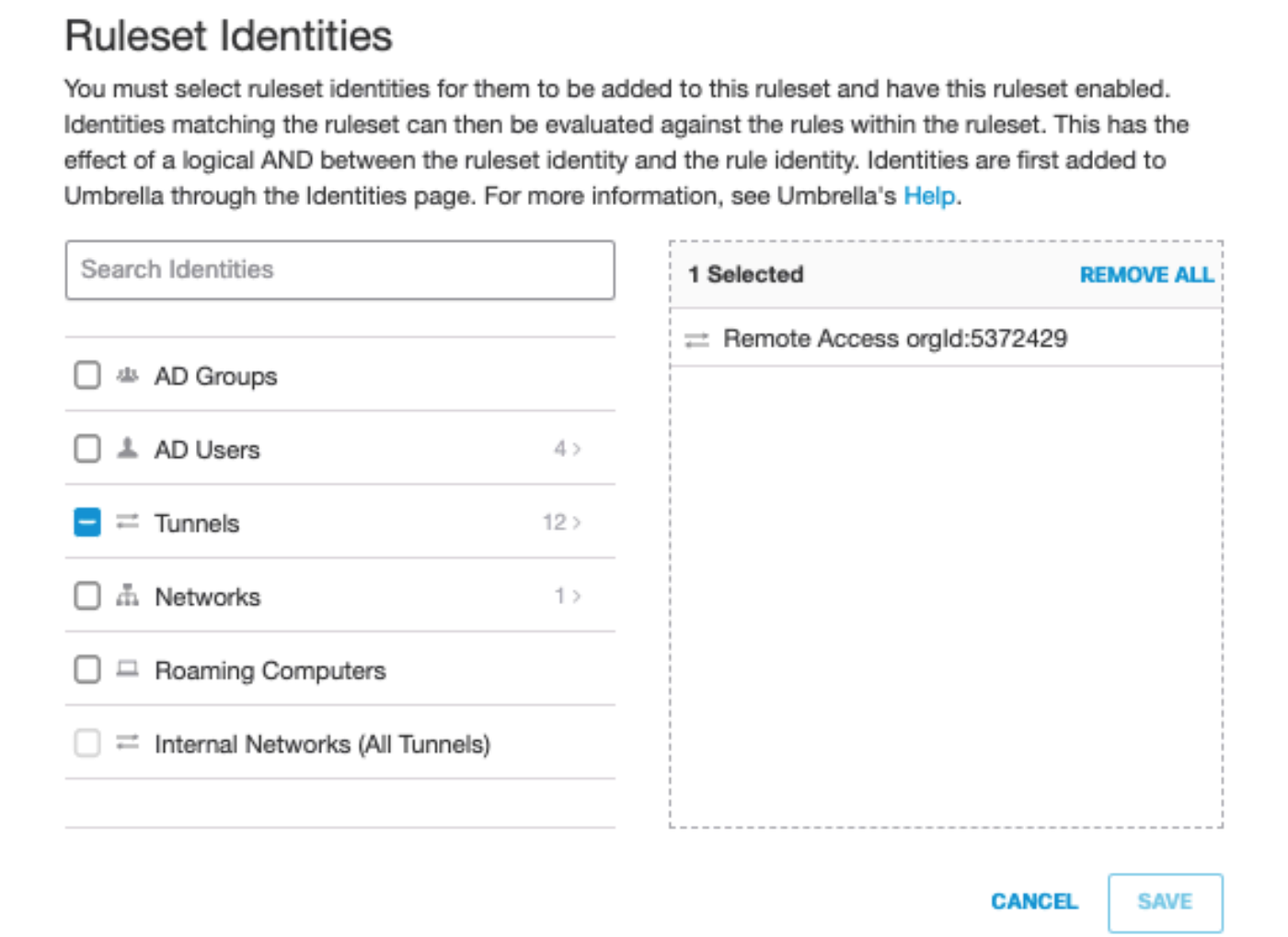
# Web策略

Web策略适用于远程访问(AnyConnect)客户端与互联网之间的流量。 根据以下文档在Deployments > Web Policies中配置规则：管理Web策略。

- Web策略不用于控制RA客户端和专用/分支Web服务器之间的访问。 Web策略仅适用于外部网站。

默认Web策略适用于远程访问客户端。 但是，我们建议创建新规则集，以专门为远程访问客户端定义安全设置。 定义规则集标识时，请从隧道列表中选择远程访问orgid:<ID> 。相同的Web策略适用于所有远程访问用户。

创建规则集后，可以添加Web规则，用于定义内容类别过滤和应用设置。




4409322363924

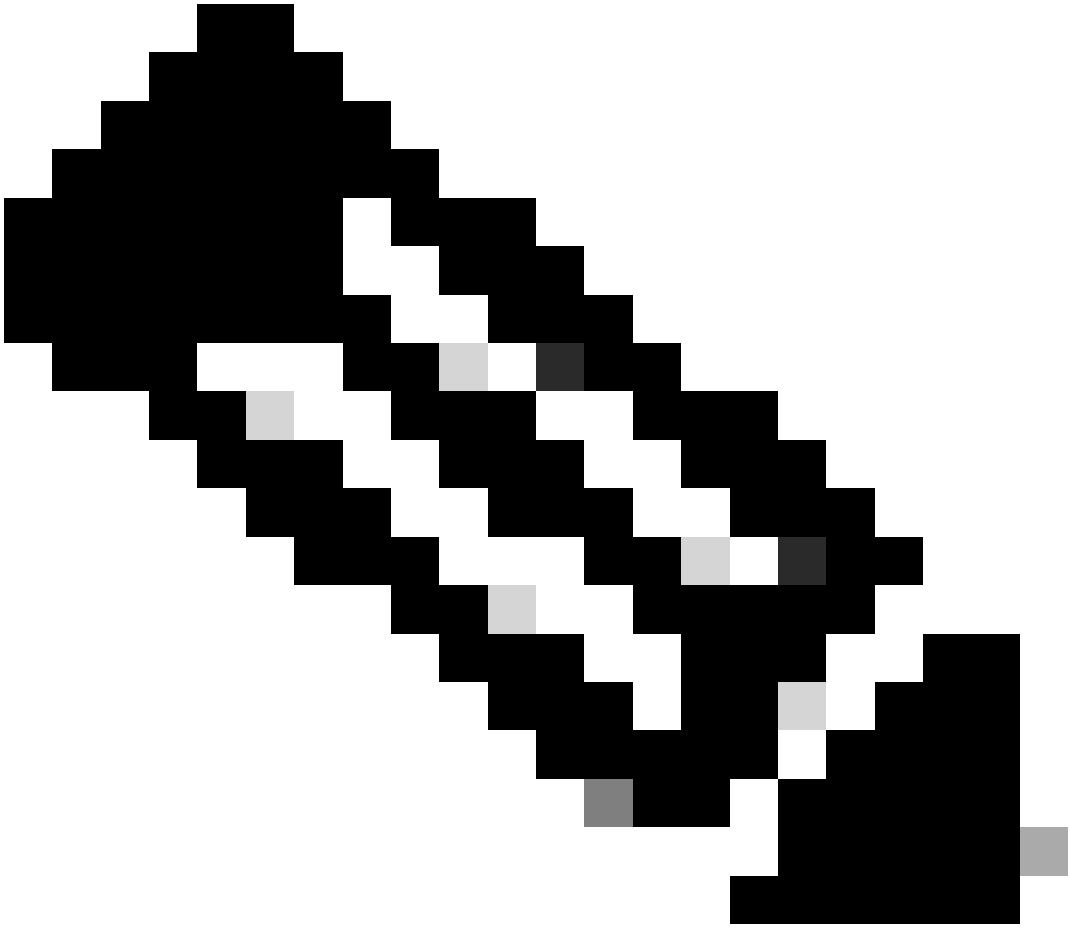
## Web用户标识

默认情况下，远程访问流量无法按用户或组进行控制。 同一策略基于“远程访问规则”身份应用于所

有RA流量。要添加用户/组标识，您有两个选项：

- 安装我们的AnyConnect Umbrella漫游安全模块并启用SWG代理功能。代理将Web流量直接发送到Umbrella SWG，并应用“漫游计算机”身份。此模块还支持可选的AD用户标识。
- 在影响“远程访问规则”身份的Web规则集中启用SAML。在连接到远程访问后，在生成Web浏览器流量时，会再次提示RA用户通过SAML进行身份验证。

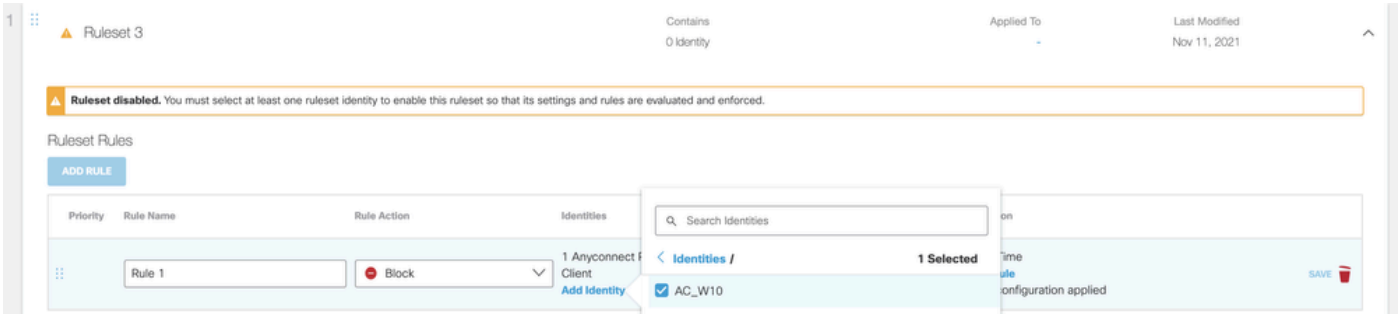
---



注意：使用Umbrella模块进行AnyConnect时，可以根据您的分割隧道配置，在隧道内部或外部发送SWG流量。

---

此示例显示如何为单个AnyConnect客户端配置DNS策略(Policies > DNS Policies) — 仅当部署了Umbrella AnyConnect漫游模块时，才可能配置该策略：



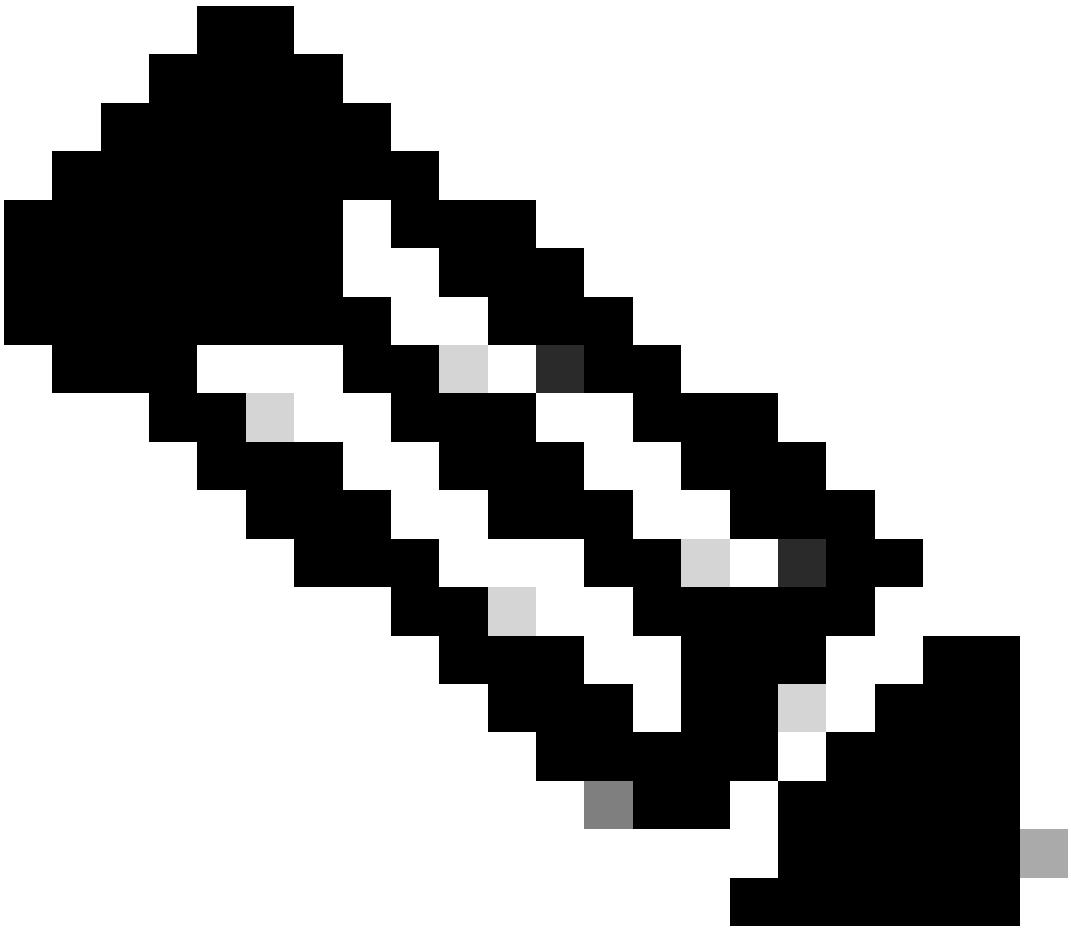

4410210499476

# DLP策略

数据丢失策略适用于远程访问(AnyConnect)客户端和互联网之间的流量。根据以下文档配置“部署>防数据丢失策略”中的规则：[管理数据保护策略](#)。

- DLP策略不用于控制RA客户端和专用/分支网络服务器之间的访问。 DLP策略仅适用于流量外部网站。

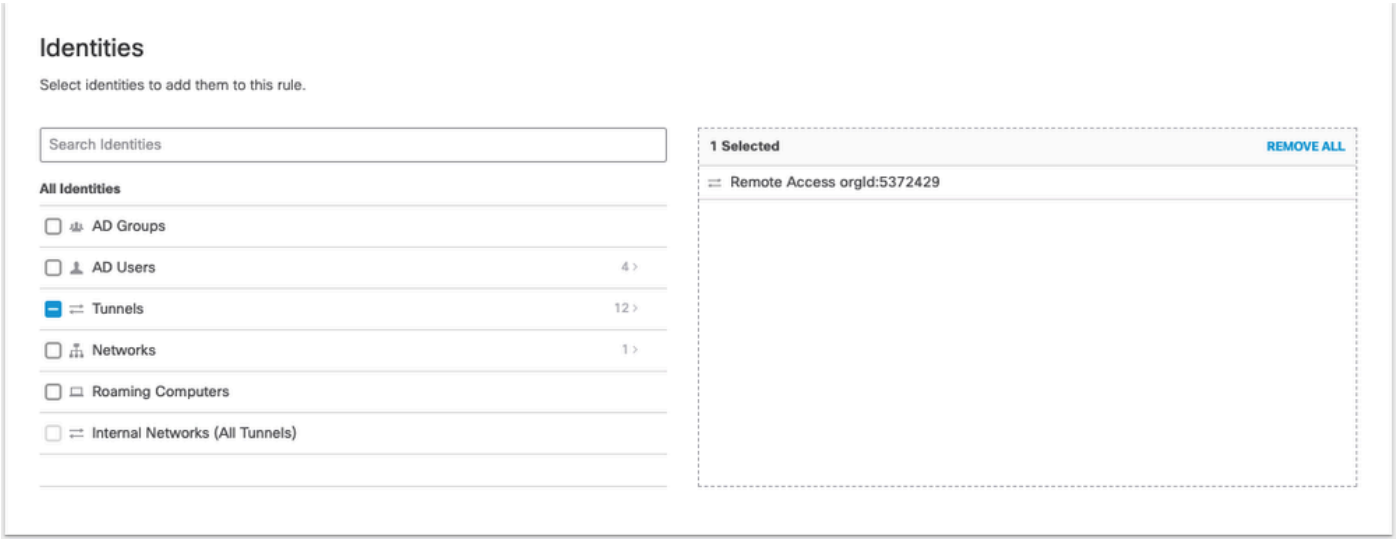
---



---

注意：要应用DLP策略，您必须首先为远程访问用户创建了一个Web规则集。Web规则集必须启用HTTPS解密。

为数据保护规则选择身份时，请选择Remote Access orgid:<ID>。相同的数据保护策略适用于所有用户。要完成DLP规则，您还需要选择或定义DLP分类器。




4409322428820

## DLP用户标识

DLP从安全Web网关（Web策略）获取用户身份。 有关如何添加用户标识的说明，请参阅Web策略部分。

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）。