DNS 策略

以下主题介绍 DNS 策略、DNS 规则，以及向受管设备部署 DNS 策略的方法。

DNS 策略概述

基于DNS的安全智能允许你根据客户端请求的域名，使用安全智能阻止列表来阻止流量。思科提供可用于过滤流量的域名情报，您还可以根据部署配置自定义域名列表和源。

DNS策略阻止列表上的流量会立即被阻止，因此不会受到任何进一步的检查--不是为了入侵、利用、恶意软件等，但也不是为了网络发现。你可以使用安全智能的不阻止列表来覆盖阻止列表并强制评估访问控制规则，而且，在被动部署中建议你使用"仅监控"设置来进行安全智能过滤。这允许系统分析本会被阻止列表阻断的连接，但也会记录与阻止列表的匹配，并生成一个连接结束的安全情报事件。

注释 基于 DNS 的安全情报可能无法为域名实现预期功能，除非 DNS 服务器由于到期删除域缓存条目，或者客户端的 DNS 缓存或本地 DNS 服务器的缓存被清除或已到期。

您可使用 DNS 策略及关联的 DNS 规则配置基于 DNS 的安全情报。要将配置部署到设备，您必须将 DNS 策略与访问控制策略相关联，然后将配置部署到受管设备。

Cisco Umbrella DNS 策略

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到Cisco Umbrella。这使 Cisco Umbrella 可以根据域名验证请求是被允许还是被阻止，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，则必须配置 Cisco Umbrella 连接，将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，您有两条防线：

- 您的本地 DNS 检测策略
- Cisco Umbrella 基于云的策略

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些标准来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

有关如何在管理中心设置 Umbrella DNS 连接器的详细信息，请参阅为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器。

DNS 策略组件

DNS 策略允许您使用阻止列表基于域名阻止连接，或使用“不阻止”列表来免除此类连接的此类阻止。以下列表介绍可在创建 DNS 策略后更改的配置。

名称和描述

每个 DSN 策略必须拥有唯一的名称。说明为可选项。

在多域部署中，策略名称在域层次结构中必须是唯一的。系统可能会识别出与您在当前域中无法查看的策略名称的冲突。

规则

规则提供一种基于域名处理网络流量的精细方法。DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。

创建 DNS 策略时，系统使用默认的全局 DNS 不阻止列表和默认的 DNS 全局阻止列表规则来填充该策略。两个规则均固定到其各自类别中的第一个位置。您无法修改这些规则，但是可以将其禁用。

在多域部署中，系统还会将后代 DNS 不阻止列表和后代 DNS 阻止列表规则添加到后代域中的 NDS 策略。这些规则固定到其各自类别中的第一个位置。

注释 如果为 管理中心启用多租户，则系统组成域的层次结构，包括祖先域和后代域。这些域截然不同并独立于 DNS 管理中所使用的域名。

后代列表包含系统子域用户的阻止或不阻止列表上的域。从祖先域中，您无法查看后代列表的内容。如果您不希望子域用户将域添加到阻止或不阻止列表：

- 禁用后代列表规则，并且
- 使用访问控制策略继承设置执行安全情报

系统按照以下顺序评估规则：

- DNS 规则的全局不阻止列表（如果启用）
- 后代 DNS 不阻止列表规则（如果启用）
- 包含不阻止操作的的规则
- DNS 规则的全局阻止列表（如果启用）
- 后代 DNS 阻止列表规则（如果启用）
- 包含除不阻止以外的操作的规则

通常，系统根据第一个 DNS 规则（其中所有规则的条件都与流量匹配）处理基于 DN 的网络流量。如果没有任何 DNS 规则与流量匹配，则系统根据关联的访问控制策略规则继续评估流量。DNS 规则条件可以简单，也可以复杂。

DNS 策略许可证要求

威胁防御 许可证

IPS

经典许可证

保护

DNS 策略的要求和必备条件

型号支持

任意

支持的域

任意

用户角色

- 管理员

- 访问管理员
- 网络管理员

管理 DNS 和 Umbrella DNS 策略

使用“DNS 策略”(DNS Policy) 页面（**策略** > **访问控制** > **DNS**）管理自定义 DNS 和 Umbrella DNS 策略。

除了您创建的自定义策略之外，系统还提供默认 DNS 策略和默认 Umbrella DNS 策略。默认 DNS 策略会使用默认阻止列表和不阻止列表。您可以编辑并使用系统提供的自定义策略。在多域部署中，默认 DNS 策略使用默认的全局 DNS 阻止列表、全局 DNS 不阻止列表、后代 DNS 阻止列表和后代 DNS 不阻止列表，并且只能在全局域中编辑。

在多域部署中，系统会显示在当前域中创建的策略，您可以对其进行编辑。系统还会显示在祖先域中创建的策略，您不可以对其进行编辑。要查看和编辑在较低域中创建的策略，请切换至该域。

过程

步骤 1 选择**策略** > **访问控制** > **DNS**。

步骤 2 要管理 DNS 策略，请执行以下操作：

- 比较 - 要比较 DNS 策略，请点击**比较策略 (Compare Policies)**，然后如比较策略中所述继续操作。
- “复制”(Copy) - 要复制 DNS 策略，请点击 **复制**（），然后如编辑 DNS 策略， 第 5 页中所述继续操作。
- “创建”(Create) - 要创建新的 Umbrella DNS 策略，请点击**新建策略 (New Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**，然后如创建 Umbrella DNS 策略， 第 17 页中所述继续操作。
- “删除”(Delete) - 要删除 DSN 或 Umbrella DSN 策略，请点击 **删除**（），然后确认要删除策略。
- “编辑”(Edit) - 要修改现有 DNS 策略，请点击 **编辑**（），然后如编辑 DNS 策略， 第 5 页中所述继续操作。要修改现有 Umbrella DNS 策略，请点击 **编辑**（），然后如编辑 Cisco Umbrella DNS 策略和规则， 第 17 页中所述继续操作。

创建基本 DNS 策略

当您创建新的 DNS 策略时，它包含默认设置。然后，您必须对其进行编辑以自定义行为。

过程

步骤 1 选择策略 > 访问控制 > DNS。

步骤 2 点击添加 DNS 策略 (Add DNS Policy) > DNS 策略 (DNS Policy)。

步骤 3 在 Name 和 Description 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击保存 (Save)。

下一步做什么

配置策略。请参阅编辑 DNS 策略，第 5 页。

编辑 DNS 策略

一个用户一次只能使用一个浏览器窗口编辑一个DNS策略。如果多个用户尝试保存同一策略，系统会仅保留第一组保存的更改。

为保护会话隐私，在策略编辑器上 30 分钟未执行任何操作之后，系统将显示警告。在 60 分钟后，系统将放弃更改。

过程

步骤 1 选择策略 > 访问控制 > DNS。

步骤 2 点击您要编辑的 DNS 策略旁边的编辑（）。

如果显示视图（），则表明配置属于祖先域，或者您没有修改配置的权限。

步骤 3 要编辑 DNS 策略，请执行以下操作：

- 名称和说明 - 要更改名称或说明，请点击相应的字段并键入新信息。
- 规则 - 要添加、分类、启用、禁用或以其他方式管理 DNS 规则，请点击规则 (Rules)，然后如创建和编辑 DNS 规则，第 6 页中所述继续操作。

步骤 4 点击保存 (Save)。

下一步做什么

- 或者，进一步配置新策略，如《Cisco Secure Firewall Management Center 管理指南》中的使用安全情报记录连接中所述。
- 部署配置更改；请参阅部署配置更改。

DNS 规则

DNS 规则根据主机请求的域名处理流量。作为安全情报的一部分，此评估发生在所有流量解密之后以及访问控制评估之前。

系统按照您指定的顺序将流量与DNS规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中规则的所有条件都与流量匹配）处理网络流量。

除其唯一名称之外，每个 DNS 规则都具有以下基本组件：

状态

默认情况下，规则处于启用状态。如果您禁用某规则，系统将不用它来评估网络流量并停止为该规则生成警告和错误。

位

DNS 策略中的规则从 1 开始进行编号。系统按升序规则编号以自上而下的顺序将流量与规则相匹配。除 Monitor 规则之外，流量匹配的第一个规则是处理该流量的规则。

条件

条件指定规则处理的特定流量。DNS 规则必须包含 DNS 源或列表条件，还可以按安全区域、网络或 VLAN 匹配流量。

操作

规则的操作确定系统如何处理匹配流量：

- 允许包含**不阻止**操作的流量，需进一步进行访问控制检查。
- 受监控的流量将根据其余有关 DNS 阻止列表的规则进行进一步评估。如果流量不匹配 DNS 阻止列表规则，则将使用访问控制规则进行检查。系统会记录流量的安全情报事件。
- 阻止列表上的流量将被丢弃，无需进一步检查。您还可以返回“找不到域”(Domain Not Found)响应，或将 DNS 查询重定向到 Sinkhole 服务器。

相关主题

关于安全情报

创建和编辑 DNS 规则

在 DNS 策略中，最多可以向阻止列表和不阻止列表规则中添加总共 32767 个 DNS 列表；即，DNS 策略中的列表数不能超过 32767。

过程

步骤 1 在 DNS 策略编辑器中，可进行以下选择：

- 要添加新规则，请点击**添加 DNS 规则 (Add DNS Rule)**。
- 要编辑现有规则，请点击 **编辑**（）。

步骤 2 输入 **Name**。

步骤 3 配置规则组成部分，或接受默认值：

- 操作 - 在**操作 (Action)** 中选择规则操作；请参阅DNS 规则操作，第 8 页。
- 条件 - 配置规则的条件；请参阅DNS 规则条件，第 9 页。
- 已启用 - 指定规则是否为**已启用 (Enabled)**。

步骤 4 点击**保存 (Save)**。

下一步做什么

- 部署配置更改；请参阅部署配置更改。

DNS 规则管理

通过 DNS 策略编辑器的**规则 (Rules)** 选项卡，您可以添加、编辑、移动、启用、禁用、删除或以其他方式管理策略中的 DNS 规则。

对于每个规则，策略编辑器会显示其名称和条件摘要，以及规则操作。其他图标代表 **警告**（）、**错误**（） 和其他重要的 **信息**（）。已禁用的规则在规则名称下方呈灰色显示并带有相应的标记 `(disabled)`。

启用和禁用 DNS 规则

创建DNS规则时，默认情况下会启用规则。如果您禁用某规则，系统将不用该规则来评估网络流量并停止为该规则生成警告和错误。查看DNS策略中的规则列表时，已禁用的规则呈灰色显示，但这些规则仍可以修改。请注意，也可使用 DNS 规则编辑器启用或禁用 DNS 规则。

过程

步骤 1 在 DNS 策略编辑器中，右键点击规则并选择规则状态。

步骤 2 点击**保存 (Save)**。

下一步做什么

- 部署配置更改。

DNS 规则顺序评估

DNS 策略中的规则从 1 开始进行编号。系统按照规则编号的升序顺序自上而下将流量与 DNS 规则相匹配。在大多数情况下，系统根据第一个DNS规则（其中所有规则的条件都与流量相匹配）处理网络流量。

- 对于“监控”(Monitor)规则，系统会记录流量，然后根据优先级较低的DNS黑名单规则继续评估流量。
- 对于“非监控”规则，在流量匹配规则后系统**不会**根据其他优先级较低的DNS规则继续评估流量。

对规则排序时，请注意：

- DNS 的全局不阻止列表 (Do-Not-Block List) 始终排在首位，优先于所有其他规则。
- 后代 DNS 白名单 (Descendant DNS 不阻止列表 (Do-Not-Block Lists) 规则仅在多域部署的非分叶域中显示。它始终排在第二位，且优先于除全局不阻止列表 (Do-Not-Block List) 之外的所有 其他规则。
- “不阻止列表”(Do-Not-Block List)部分优先于“阻止列表”(Block List)部分；不阻止列表规则始终优先于其他规则。
- “全局阻止列表”(Global Block List)始终排在“阻止列表” (Block List)部分的第一个位置，并且优先于所有其他“监控”(Monitor)和“阻止”(Block)列表规则。
- “后代 DNS 阻止列表”(Descendant DNS Block Lists)规则仅在多域部署的非分叶域中显示。它在“阻止列表”(Block List)部分中始终排在第二位，并且优先于除“全局阻止列表”(Global Block List)以外的所有其他“监控”(Monitor)和“阻止”(Block)列表规则。
- “阻止列表”(Block List)部分包含监控和阻止列表规则。
- 首次创建 DNS 规则时，如果分配**不阻止 (Do Not Block)** 操作，系统会将其放在“不阻止列表”(Do-Not-Block List)部分的最后；如果分配任何其他操作，模块会将其放在“阻止列表”(Block List)部分的最后。

可以通过拖放规则来为规则重新排序。

DNS 规则操作

每个 DNS 规则都有确定匹配流量的以下过程的操作：

- 处理 - 首先，规则操作可管理系统是否会根据阻止或不阻止列表来阻止、不阻止或监控符合规则条件的流量。
- 日志记录 - 该规则操作确定何时以及如何记录有关匹配的流量的详细信息

不阻止操作

不阻止 (Do Not Block) 操作将允许流量传递到下一个检查阶段，即访问控制规则。

系统不会记录不阻止列表匹配项。是否记录这些连接取决于其最终的安全状态。

“监控”(Monitor) 操作

监控 (Monitor) 操作旨在强制执行连接日志记录；匹配的流量既不会被立即允许，也不会被阻止。更确切地是，根据其他规则匹配流量以确定允许还是拒绝该流量。所匹配的第一个非“监控”(Monitor) DNS 规则可确定系统是否阻止流量。如果没有其他匹配的规则，流量会进行访问控制评估。

对于 DNS 策略监控的连接，系统会记录连接结束的安全情报和 管理中心数据库的连接事件。

阻止操作

这些操作会阻止流量，无需任何类型的进一步检查：

- **丢弃 (Drop)** 操作会丢弃流量。
- **找不到域 (Domain Not Found)** 操作会针对 DNS 查询返回“不存在的互联网域”响应，防止客户端解析 DNS 请求。
- **Sinkhole** 操作会返回 Sinkhole 对象的 IPv4 或 IPv6 地址以响应 DNS 查询（仅限 A 和 AAAA 记录）。Sinkhole 服务器可以记录或记录并阻止 IP 地址的后续连接。如果配置 **Sinkhole** 操作，还必须配置 Sinkhole 对象。

对于根据**丢弃 (Drop)** 或**找不到域 (Domain Not Found)** 操作而被阻止的连接，系统会记录连接开始的安全情报和连接事件。因为被阻止的流量会被立即拒绝，无需进一步检测，所以，没有要记录的唯一连接终止。

对于根据 **Sinkhole** 操作阻止的连接，日志记录取决于 Sinkhole 对象配置。如果将 Sinkhole 对象配置为仅记录 Sinkhole 连接，则系统会记录后续连接的连接结束的连接事件。如果将 Sinkhole 对象配置为记录并阻止 Sinkhole 连接，则系统会记录后续连接的连接开始的连接事件，然后阻止该连接。

DNS 规则条件

DNS 规则的条件识别该规则处理的流量的类型。条件可以简单，也可以复杂。您必须在 DNS 规则中定义 DNS 源或列表条件。还可以选择按安全区域、网络或 VLAN 控制流量。

将条件添加到 DNS 规则时：

- 如果不为规则配置特定条件，系统将不基于此标准匹配流量。
- 您可以为每个规则配置多个条件。为使规则应用于流量，流量必须匹配规则中的**所有**条件。例如，包含 DNS 源或列表条件和网络条件，但没有 VLAN 标记条件的规则会根据域名以及源或目标评估流量，无论会话采用任何 VLAN 标记。
- 最多可以为规则中的每个条件添加50个标准。匹配**所有**条件的标准的流量满足该条件。例如，您可以使用单一规则根据最多 50 个 DNS 列表和源来阻止流量。

相关主题

安全区域规则条件，第 10 页
网络规则条件
VLAN 标记规则条件
DNS 规则条件，第 11 页

安全区域规则条件

安全区域可对网络进行分段，以通过跨多个设备将接口分组来帮助管理和分类流量。

区域规则条件可根据其源和目标安全区域控制流量。如果将源区域和目标区域均添加到区域条件中，则匹配流量必须源自其中一个源区域的接口，并通过其中一个目标区域的接口流出。

正如区域中的所有接口都必须为同一类型（均为内联、被动、交换或路由），区域条件中使用的所有区域也必须为同一类型。由于被动部署的设备不会传输流量，因此不能使用具有被动接口的区域作为目标区域。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

提示 按区域限制规则是提高系统性能的一种最佳方式。如果规则不适用于通过设备任意接口的流量，则该规则不影响该设备的性能。

安全区域条件和多租户

在多域部署中，在祖先域中创建的区域可以包含位于不同域中的设备上的接口。在后代域中配置区域条件时，您的配置仅适用于可以看到的接口。

网络规则条件

网络规则条件使用内部报头按流量的源和目标 IP 地址来控制流量。使用外部报头的隧道规则具有隧道终端条件而不是网络条件。

您可以使用预定义对象构建网络条件，或手动指定单个 IP 地址或地址块。

注释 您 不能 在身份规则中使用 FDQN 网络对象。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

尽可能将匹配条件留空，尤其是安全区、网络对象和端口对象的匹配条件。指定多个条件时，系统必须匹配您指定的条件内容的各组合。

VLAN 标记规则条件

注释 访问规则中的 VLAN 标记仅适用于内联集。带 VLAN 标记的访问规则与防火墙接口上的流量不匹配。

VLAN 规则条件可控制 VLAN 标记的流量，包括 Q-in-Q（堆栈 VLAN）流量。系统使用最内层的 VLAN 标记过滤 VLAN 流量，但不包括预过滤器策略，因为它在其规则中使用最外层的 VLAN 标记。

请注意以下 Q-in-Q 支持：

- Firepower 4100/9300 上的威胁防御 -不支持 Q-in-Q （仅支持一个 VLAN 标记）。
- 所有其他型号上的威胁防御 ：
  - 内联集和被动接口-支持 Q-in-Q，最多2个 VLAN 标记。
  - 防火墙接口-不支持 Q-in-Q （仅支持一个 VLAN 标记）。

可以使用预定义对象构建 VLAN 条件，或手动输入从 1 到 4094 之间的任意 VLAN 标记。使用连字符可指定 VLAN 标记范围。

最多可以指定 50 个 VLAN 条件。

在集群中，如果遇到 VLAN 匹配问题，请编辑访问控制策略高级选项“传输/网络预处理器设置”(Transport/Network Preprocessor Settings)，然后选择**跟踪连接时忽略 VLAN 信头 (Ignore the VLAN header when tracking connections)** 选项。

注释 系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

DNS 规则条件

如果 DNS 列表、源或类别包含客户端请求的域名，则 DNS 规则中的 DNS 条件可用于控制流量。您必须在 DNS 规则中定义 DNS 条件。

无论向 DNS 条件中添加全局或自定义阻止还是不阻止列表，系统都会将所配置的规则操作应用于流量。例如，如果向规则中添加全局不阻止列表，并配置**丢弃 (Drop)** 操作，则系统会阻止所有本应被允许进入下一阶段检查的流量。

如何创建 DNS 规则

以下主题讨论如何创建 DNS 规则。

相关主题

根据 DNS 和安全区域控制流量，第 12 页
根据 DNS 和网络控制流量，第 12 页
根据 DNS 和 VLAN 控制流量，第 13 页
根据 DNS 列表或源来控制流量，第 14 页

根据 DNS 和安全区域控制流量

通过DNS规则中的区域条件，您可以根据其源安全区域来控制流量。安全区域是一个或多个接口的分组，可位于多个设备之间。

过程

步骤 1 在 DNS 规则编辑器中，点击**区域 (Zones)**。

步骤 2 从 **Available Zones** 中查找并选择您想要添加的区域。要搜索需要添加的区域，请点击 **Available Zones** 列表上方的 **Search by name** 提示，然后键入区域名称。该列表会在您键入内容时进行更新，以显示匹配的区域。

步骤 3 点击选择一个区域，或右键点击，然后选择**全选 (Select All)**。

步骤 4 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 5 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

根据 DNS 和网络控制流量

DNS 规则中的网络条件可以根据源 IP 地址控制流量。您可以为要控制的流量显式指定源 IP 地址。

过程

步骤 1 在 DNS 规则编辑器中，点击**网络 (Networks)**。

步骤 2 从 **Available Networks** 中查找并选择您想要添加的网络，如下所示：

- 要即时添加可随后添加到条件中的网络对象，请点击**可用网络 (Available Networks)** 列表上方的**添加**（＋），然后如创建网络对象中所述继续操作。
- 要搜索要添加的网络对象，请点击**可用网络**列表上方的**按名称或值搜索**提示，然后键入对象名称或对象的其中一个组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到源 (Add to Source)**，或进行拖放操作。

步骤 4 添加要手动指定的任何源 IP 地址或地址块。点击**源网络 (Source Networks)** 列表下方的**输入 IP 地址 (Enter an IP address)** 提示，然后键入 IP 地址或地址块，并点击**添加 (Add)**。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 IP 地址限制此配置可能会出现意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

根据 DNS 和 VLAN 控制流量

通过 DNS 规则中的 VLAN 条件，您可以控制 VLAN 标记流量。系统使用最内部的 VLAN 标记来按照 VLAN 识别数据包。

构建基于 VLAN 的 DNS 规则条件时，可以手动指定 VLAN 标记。或者，也可以使用 VLAN 标记对象配置 VLAN 条件，这些对象可重用，并会将名称与一个或多个 VLAN 标记相关联。

过程

步骤 1 在 DNS 规则编辑器中，选择 **VLAN 标记 (VLAN Tags)**。

步骤 2 查找并选择您要从 **Available VLAN Tags** 添加的 VLAN，如下所述：

- 要即时添加可随后添加到条件中的 VLAN 标记，请点击“可用 VLAN 标记”(Available VLAN Tags) 列表上方的 **添加**（＋） 并继续操作，如创建 VLAN 标记对象中所述。
- 要搜索将添加的 VLAN 标记对象和组，请点击 **Available VLAN Tags** 列表上方的 **Search by name or value** 提示，然后键入对象的名称或对象中 VLAN 标记的值。列表会在您键入内容时进行更新，以显示匹配的对象。

步骤 3 点击**添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 添加要手动指定的任何 VLAN 标记。点击**所选 VLAN 标记 (Selected VLAN Tags)** 列表下方的**输入 VLAN 标记 (Enter a VLAN Tag)** 提示，然后键入 VLAN 标记或范围并点击**添加 (Add)**。您可以指定介于 1 和 4094 之间的任何 VLAN 标记；使用连字符指定 VLAN 标记的范围。

系统会为每个枝叶域构建单独的网络映射。在多域部署中，使用文字 VLAN 标记限制此配置可产生意外结果。 通过使用支持覆盖的对象，后代域管理员可为其本地环境自定义全局配置。

步骤 5 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

根据 DNS 列表或源来控制流量

过程

步骤 1 在 DNS 规则编辑器中，点击 **DNS**。

步骤 2 从 **DNS 列表和源 (DNS Lists and Feeds)** 中查找并选择要添加的 DNS 列表和源，如下所示：

- 要动态添加可随后添加到条件中的 DNS 列表和源，请点击 **DNS 列表和源 (DNS Lists and Feeds)** 列表上方的 **添加**（＋），然后如创建安全情报源中所述继续操作。
- 要搜索将添加的 DNS 列表、源或类别，请点击 **DNS 列表和源** 列表上方的 **按名称或值搜索** 提示，然后键入对象名称或其中一个对象的组件的值。列表会在您键入内容时进行更新，以显示匹配的对象。
- 有关系统提供的威胁类别的说明，请参阅安全情报类别。

步骤 3 点击 **添加到规则 (Add to Rule)**，或进行拖放操作。

步骤 4 保存或继续编辑规则。

下一步做什么

- 部署配置更改。

DNS 策略部署

完成 DNS 策略配置更新后，您必须将其部署为访问控制配置的一部分。

- 将 DNS 策略与访问控制策略相关联，如配置安全情报中所述。
- 部署配置更改。

Cisco Umbrella DNS 策略

管理中心中的 Cisco Umbrella DNS 连接有助于将 DNS 查询重定向到Cisco Umbrella。这使 Cisco Umbrella 可以根据域名验证请求是被允许还是被阻止，并对请求应用基于 DNS 的安全策略。如果使用 Cisco Umbrella，则必须配置 Cisco Umbrella 连接，将 DNS 查询重定向到 Cisco Umbrella。

Umbrella 连接器是系统 DNS 检测的一部分。如果现有 DNS 检测策略映射决定根据 DNS 检测设置阻止或丢弃请求，则该请求不会转发至思科 Umbrella。因此，您有两条防线：

- 您的本地 DNS 检测策略
- Cisco Umbrella 基于云的策略

将 DNS 查询请求重定向到思科 Umbrella 时，Umbrella 连接器会添加 EDNS （DNS 扩展机制） 记录。EDNS 记录包括设备标识符信息、 组织 ID 和客户端 IP 地址。基于云的策略可以使用 FQDN 信誉以及这些标准来控制访问。还可以选择使用 DNSCrypt 加密 DNS 请求，以确保用户名和内部 IP 地址的隐私性。

有关如何在管理中心设置 Umbrella DNS 连接器的详细信息，请参阅为 Cisco Secure Firewall Management Center 配置 Umbrella DNS 连接器。

如何将 DNS 请求重定向到 Cisco Umbrella

本节提供使用 管理中心 将 DNS 请求从设备重定向到 Cisco Umbrella 的说明。

步骤	相应操作	更多信息
1	确保您已满足前提条件。	配置 Umbrella DNS 连接器的前提条件， 第 15 页
2	配置 Cisco Umbrella 连接设置。	配置 Cisco Umbrella 连接设置， 第 16 页
3	创建 Umbrella DNS 策略	创建 Umbrella DNS 策略， 第 17 页
4	配置 Umbrella DNS 策略	编辑 Cisco Umbrella DNS 策略和规则， 第 17 页
5	将 Umbrella DNS 策略与访问控制策略相关联	将 Umbrella DNS 策略与访问控制策略相关联， 第 18 页

配置 Umbrella DNS 连接器的前提条件

表 *1:* 支持的最低平台

Product	版本
Cisco Secure Firewall Threat Defense	6.6 及更高版本
Cisco Secure Firewall Management Center	7.2 及更高版本

- 在 https://umbrella.cisco.com上建立 Cisco Umbrella 帐户，然后在 http://login.umbrella.com上登录 Umbrella。
- 将 CA 证书从 Cisco Umbrella 服务器导入 管理中心。在 Cisco Umbrella 中，选择**部署 (Deployments)** > **配置 (Configuration)** > **根证书 (Root Certificate)** 并下载证书。

必须导入根证书，才能与思科 Umbrella 注册服务器建立 HTTPS 连接。证书需要受信任才能进行 SSL 服务器验证，这是管理中心中的非默认选项。将设备的证书复制并粘贴到 管理中心（**设备 (Device) > 证书 (Certificates)**）中。

- 在设备上安装证书。
- 从 Umbrella 获取以下数据：
  - 组织 ID
  - 网络设备密钥
  - 网络设备密钥
  - 旧版网络设备令牌
- 确保 管理中心 已连接到互联网。
- 确保已在 管理中心 中启用具有出口控制功能选项的基础许可证。
- 确保配置 DNS 服务器以解析 api.opendns.com。
- 确保 管理中心 可以解析 management.api.umbrella.com 以进行策略配置。
- 配置到 api.opendns.com 的 威胁防御 路由。

配置 Cisco Umbrella 连接设置

思科 Umbrella 连接设置定义了在思科 Umbrella 中注册设备时所需的 API 令牌。

开始之前

使用思科 Umbrella https://umbrella.cisco.com 建立账户，然后通过 https://dashboard.umbrella.com 登录 Umbrella，获取与思科 Umbrella 建立连接所需的信息。

过程

步骤 1 选择**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **思科 Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 2 获取以下详细信息并将其添加到**常规 (General)** 设置中：

- **组织 ID (Organization ID)** - 在思科 Umbrella 上标识您的组织的唯一编号。每个 Umbrella 组织都是一个单独的 Umbrella 实例，并且有自己的控制面板。组织通过其名称和组织 ID（组织 ID）进行标识。
- **网络设备密钥 (Network Device Key)** - 从思科 Umbrella 获取 Umbrella 策略的密钥。
- **网络设备密钥 (Network Device Secret)** - 从思科 Umbrella 获取 Umbrella 策略的密钥。

- **传统网络设备令牌 (Legacy Network Device Token)** - 通过思科 Umbrella 控制面板颁发 Umbrella 传统网络设备 API 令牌。Umbrella 需要 API 令牌才能注册网络设备。

步骤 3 在**高级 (Advanced)** 下，配置以下可选设置：

- **DNSCrypt 公钥 (DNSCrypt Public Key)** - DNSCrypt 对终端和 DNS 服务器之间的 DNS 查询进行身份验证和加密。要启用 DNScrypt，您可以为证书验证配置 DNScrypt 公钥。密钥是一个 32 字节的十六进制值，预配置为 B735:1140:206F:225d:3E2B:d822:D7FD:691e:A1C3:3cc8:D666:8d0c:BE04:bfab:CA43:FB79，即公钥的 Umbrella 任播服务器。
- **管理密钥 (Management Key)** - 从 Umbrella 云获取 VPN 策略的数据中心详细信息的密钥。
- **管理秘密 (Management Secret)** - 用于从 Umbrella 云获取 VPN 数据中心的秘密。

步骤 4 点击**测试连接 (Test Connection)** - 测试是否可从 管理中心 访问 Cisco Umbrella Cloud。在提供所需的组织 ID 和网络设备详细信息时，您会创建 Umbrella 连接。

步骤 5 点击**保存 (Save)**。

创建 Umbrella DNS 策略

过程

步骤 1 选择**策略** > **访问控制** > **DNS**。

步骤 2 点击**添加 DNS 策略 (Add DNS Policy)** > **Umbrella DNS 策略 (Umbrella DNS Policy)**。

步骤 3 在 **Name** 和 **Description** 中为策略提供唯一名称和说明（后者为可选项）。

步骤 4 点击**保存 (Save)**。

下一步做什么

配置策略。请参阅编辑 Cisco Umbrella DNS 策略和规则，第 17 页。

编辑 Cisco Umbrella DNS 策略和规则

过程

步骤 1 选择**策略** > **访问控制** > **DNS**。

步骤 2 在“DNS 策略”(DNS Policy) 页面上，选择要编辑的 Umbrella DNS 策略，然后点击 **编辑**（✎）。

刷新 **Umbrella** 保护策略

如果要从思科 Umbrella 获取最新的 Umbrella 保护策略，请点击**上次更新 Umbrella 保护策略 (Umbrella Protection Policy Last Updated)** 旁边的**刷新 (Refresh)** 图标。

要配置或修改管理中心的 Umbrella 连接设置，请转至**集成 (Integration)** > **其他集成 (Other Integrations)** > **云服务 (Cloud Services)** > **思科 Umbrella 连接 (Cisco Umbrella Connection)**。

步骤 3 在 Cisco Umbrella DNS 策略编辑器中，选择 Umbrella DNS 规则并点击 **编辑**（✎）。

步骤 4 配置规则组成部分，或接受默认值：

- **Umbrella 保护策略 (Umbrella Protection Policy)** - 指定要应用于设备的思科 Umbrella 策略的名称。
- **绕过域 (Bypass Domain)** - 指定 DNS 请求应绕过思科 Umbrella 直接转至所配置的 DNS 服务器的本地域。

  例如，假设允许所有内部连接，可以借助内部 DNS 服务器解析组织域名的所有名称。
- **DNSCrypt** - 启用 DNSCrypt，以便为设备和思科 Umbrella 之间的连接加密。

  启用 DNScrypt 将使用 Umbrella 解析器启动密钥交换线程。密钥交换线程每小时执行与解析器的握手，并使用新密钥来更新设备。由于 DNScrypt 使用 UDP/443，您必须确保用于 DNS 检测的类映射包含该端口。请注意，默认检测类已在 DNS 检测中包括 UDP/443。
- **空闲超时 (Idle Timeout)** - 配置当服务器没有响应时，在删除从客户端至 Umbrella 服务器的连接之前的空闲超时。

步骤 5 点击**保存 (Save)**。

下一步做什么

将 Umbrella DNS 策略与访问控制策略相关联有关详细信息，请参阅将 Umbrella DNS 策略与访问控制策略相关联，第 18 页。

将 Umbrella DNS 策略与访问控制策略相关联

在设备上部署 Umbrella DNS 策略之前，必须将其与访问控制策略相关联。

过程

步骤 1 选择**策略 (Policies) 访问控制 (Access Control)**，然后选择要编辑的访问策略。

步骤 2 选择**安全智能 (Security Intelligence)**。

步骤 3 从 **Umbrella DNS 策略 (Umbrella DNS Policy)** 下拉列表中选择 Umbrella DNS 策略。

步骤 4 点击**保存 (Save)**。

下一步做什么

部署配置更改；请参阅部署配置更改。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。