思科 Umbrella

您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的 FQDN 策略应用于用户连接。以下主题介绍如何配置 Umbrella 连接器将设备与思科 Umbrella 进行集成。

关于思科 Umbrella 连接器

如果使用思科 Umbrella，可以配置思科 Umbrella 连接器，将 DNS 查询重定向到思科 Umbrella。这样，Cisco Umbrella 就能识别对未经允许或有问题的域名的请求，并应用基于 DNS 的安全策略。

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，有两条保护防线：本地 DNS 检测策略和 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 信誉以及这些条件来控制访问。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。

思科 Umbrella 企业安全策略

在基于云的思科 Umbrella 企业安全策略中，可以基于 DNS 查询请求中的完全限定域名 (FQDN) 的信誉来控制访问。企业安全策略可以强制执行以下操作之一：

- 允许 - 如果对某个 FQDN 未设置阻止规则，并且 Cisco Umbrellaa 确定其属于非恶意站点，则系统会返回该站点的实际 IP 地址。这是正常的 DNS 查询行为。

- 代理 - 如果对某个 FQDN 未设置阻止规则，并且 Cisco Umbrellaa 确定其属于恶意站点，则 DNS 应答会返回 Umbrella 智能代理的 IP 地址。然后，该代理可以检查 HTTP 连接，并应用 URL 过滤。必须确保从 Cisco Umbrellaa 控制面板（**安全设置 (Security Setting)** > **启用智能代理 (Enable Intelligent Proxy)**）启用智能代理。
- 阻止 - 如果明确阻止 FQDN，或 Cisco Umbrellaa 确定其属于恶意站点，则 DNS 应答会返回已阻止连接的 Umbrella 云登录页面的 IP 地址。

思科 Umbrella 注册

在设备上配置 Umbrella 连接器时，它会在云中向思科 Umbrella 注册。在注册流程中，分配设备 ID，用于确定以下任一项：

- 单情景模式下的一个独立设备。
- 单情景模式下的一个高可用性对。
- 单情景模式下的一个集群。
- 多情景独立设备中的一个安全情景。
- 高可用性对的一个安全情景。
- 集群的一个安全情景。

注册后，设备详细信息将显示在思科 Umbrella 控制面板上。然后，可以更改向设备附加的策略。在注册期间，使用配置中指定的策略，或者分配默认策略。可以向多个设备分配同一 Umbrella 策略。指定策略后收到的设备 ID 不同于未指定策略情况下收到的设备 ID。

从旧版 API 令牌切换到 API/密钥

从 ASA 9.23(1) 开始，Umbrella 将 API 注册机制从 API 令牌更改为 API 密钥和秘密。如果使用的是旧版令牌，则可通过执行以下操作从旧版 API 切换到 API/密钥 API。详细步骤请参见相关程序。

过程

步骤 1 导入新 API 的证书。您需要安装 ISRG Root X1 自签名证书。

步骤 2 禁用 Umbrella。

步骤 3 删除现有的令牌注册。

步骤 4 配置新的 API 和密钥。

步骤 5 重新启用 Umbrella。

思科 Umbrella 连接器的许可要求

要使用思科 Umbrella 连接器，必须拥有 3DES 许可证。如果正在使用智能许可，必须启用账户的导出控制功能。

思科 Umbrella 门户具有单独的许可要求。

思科 Umbrella 的准则和限制

情景模式

- 在多情景模式下，可在每个情景下配置 Umbrella 连接器。每个情景都有单独的设备 ID，并且在思科 Umbrella 连接器控制面板中被表示为独立设备。设备名称是在情景中配置的主机名，再加上硬件型号和情景名称。例如，CiscoASA-ASA5515-Context1。

故障转移

- 高可用性对中的主用设备向思科 Umbrella 将此高可用性对注册为单一设备。两个对等体使用根据其序列号形成的同一设备 ID：*primary-serial-number_secondary-serial-number*。对于多情景模式，安全情景的每一对都被视为单一设备。启用思科 Umbrella 前，必须配置高可用性，并且设备必须成功建立高可用性组 （即使备用设备目前处于故障状态），否则注册将以失败告终。

集群

- 集群控制单元在 Cisco Umbrellaa 中作为单一设备注册该集群。所有对等体使用同一设备 ID。对于多情景模式，该集群中的安全情景在所有对等体中均被视为单一设备。

其他准则

- 仅直通流量中的 DNS 请求重定向到思科 Umbrella。系统自身发起的 DNS 请求永远不会重定向到思科 Umbrella。例如，基于 FQDN 的访问控制规则以及其他命令或配置设置中使用的任何 FQDN 永远无法根据 Umbrella 策略解析。
- 思科 Umbrella 连接器适用于直通流量中任何 DNS 请求。然而，只有 DNS 响应用于 HTTP/HTTPS 连接时，阻止和代理操作才有效，因为返回的 IP 地址是针对网站的。非 HTTP/HTTPS 连接的任何列入阻止和代理地址的操作将失败或以误导性方式完成。例如，针对列入阻止 FQDN 执行 ping 操作会导致对托管 Cisco Umbrellaa 云阻止页面的服务器执行 ping 操作。

注释 Cisco Umbrella 试图智能地识别可能是非 HTTP/HTTPS 的 FQDN，并且对于代理域名的 FQDN，不向智能代理返回 IP 地址。

- 系统仅向思科 Umbrella 发送 DNS/UDP 流量。如果启用 DNS/TCP 检测，则系统不会向思科 Umbrella 发送任何 DNS/TCP 请求。然而，DNS/TCP 请求不会增加 Umbrella 旁路计数器的读数。
- 如果启用 Umbrella DNScrypt 检测，则系统会使用 UDP/443 进行加密会话。必须将 UDP/443 和 UDP/53 包含在为思科 Umbrella 应用 DNS 检测的类映射中，以确保 DNScrypt 正常运行。UDP/443 和 UDP/53 均包含在 DNS 的默认检测类中，但如果创建一个自定义类，请确保所定义的 ACL 将这两个端口都包含到匹配类中。
- DNScrypt 仅对证书更新握手使用 IPv4。但是，DNSscrypt 会加密 IPv4 和 IPv6 流量。
- 必须有一个 IPv4 路由可到达互联网 api.umbrella.com 和 api.opendns.com（注册仅使用 IPv4）。同时，还必须有到以下 DNS 解析器的路由，且访问规则必须允许流向这些主机的 DNS 流量。这些路由可以经过数据接口或管理接口；任何有效路由均适用于注册和 DNS 解析。系统会指示系统使用的默认服务器；通过在 Umbrella 全局设置中配置解析器，可以使用其他服务器。
  - 208.67.220.220 （IPv4 的系统默认值）
  - 208.67.222.222
  - 2620:119:53::53 （IPv6 的系统默认值）
  - 2620:119:35::35
- 系统不支持 Umbrella FamilyShield 服务。如果配置 FamilyShield 解析器，则可能会出现意外结果。
- 当评估是否在故障时打开时，系统会判断 Umbrella 解析器是否关闭，或干预设备是否根据发送 DNS 请求后等待的时间长度来丢弃 DNS 请求或响应。系统不考虑其他因素，例如没有到 Umbrella 解析器的路由。
- 要取消注册设备，请先删除 Umbrella 配置，然后从思科 Umbrella 控制面板中删除设备。
- 使用 IP 地址而不使用 FQDN 的任何 Web 请求均会绕过思科 Umbrella。此外，如果漫游客户端从不同于通过启用 Umbrella 的设备的 WAN 连接获取 DNS 解析，则使用这些解析的连接将绕过思科 Umbrella。
- 如果用户具有 HTTP 代理，则该代理可能会执行 DNS 解析，并且解析不会通过思科 Umbrella。
- 不支持 NAT DNS46 和 DNS64。无法在 IPv4 与 IPv6 寻址之间转换 DNS 请求。
- EDNS 记录将同时包括 IPv4 和 IPv6 主机地址。
- 如果客户端使用基于 HTTPS 的 DNS，云安全服务将不会检测 DNS 和 HTTP/HTTPS 流量。

配置思科 Umbrella 连接器

可以配置设备，以与云中的思科 Umbrella 交互。系统将 DNS 查询请求重定向到思科 Umbrella，由后者应用基于云的企业级安全性完全限定域名 (FQDN) 策略。对于恶意或可疑流量，可以从站点阻止用户或将其重定向至可以根据基于云的策略执行 URL 过滤的智能代理。

以下程序介绍用于配置思科 Umbrella 连接器的　端到端流程。

开始之前

在多情景模式下，请在应使用思科 Umbrella 的每个安全情景中执行此程序。

过程

步骤 1 在思科 Umbrella（地址：https://umbrella.cisco.com）上建立账户。

步骤 2 从思科 Umbrella 注册服务器安装 CA 证书，第 5 页.

设备注册使用 HTTPS，这要求安装根证书。

步骤 3 如果尚未启用，则配置 DNS 服务器，并在接口上启用 DNS 查询。

可以使用自己的服务器，或配置思科 Umbrella 服务器。即使配置其他服务器，DNS 检测也会自动重定向到思科 Umbrella 解析器。

- 208.67.220.220
- 208.67.222.222
- 2620:119:53::53
- 2620:119:35::35

示例：

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220
```

步骤 4 配置 Umbrella 连接器全局设置，第 6 页。

步骤 5 在 DNS 检测策略映射中启用 Umbrella，第 9 页。

步骤 6 验证 Umbrella 注册，第 10 页。

从思科 Umbrella 注册服务器安装 CA 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。注册设备时，系统使用 HTTPS 连接。在 Cisco Umbrellaa 中，依次选择 **部署 (Deployments) > 配置 (Configuration) > 根证书 (Root Certificate)** 并下载证书。

使用 API 和密钥注册 Umbrella 时，需要安装 ISRG Root X1 自签名证书 pem 文件。您可以从 https://letsencrypt.org/certs/isrgrootx1.pem 获取此证书。

开始之前

如果 Umbrella 更新了证书，则您需要下载新证书。根证书也可能发生变化。确保上传了正确的根证书。

更新证书时，必须先禁用 Umbrella，然后再启用，这样系统才能接收新证书并正确注册 Umbrella。

过程

步骤 1 为思科 Umbrella 注册服务器创建信任点。

crypto ca trustpoint *name*

可以使用您希望使用的任何名称命名信任点（最多 128 个字符），例如 ctx1 或 umbrella_server。

示例：

```
ciscoasa(config)# crypto ca trustpoint ctx1
ciscoasa(config-ca-trustpoint)#
```

步骤 2 指出您想要通过粘贴证书手动注册。

enrollment terminal

示例：

```
ciscoasa(config-ca-trustpoint)# enrollment terminal
ciscoasa(config-ca-trustpoint)#
```

步骤 3 导入证书。

crypto ca authenticate *name*

输入为此证书创建的信任点的名称。根据提示操作并粘贴 Base-64 编码证书。不要包括 BEGIN CERTIFICATE 和 END CERTIFICATE 行。

```
ciscoasa(config-ca-trustpoint)# crypto ca authenticate ctx1
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
```

配置 Umbrella 连接器全局设置

Umbrella 全局设置主要定义在 Cisco Umbrella 注册设备所需的 API 和密钥或旧版 API 令牌。

全局设置不足以启用 Umbrella。您还必须在 DNS 检测策略映射中启用 Umbrella，如 在 DNS 检测策略映射中启用 Umbrella，第 9 页 所述。

开始之前

- 登录 Umbrella 控制面板并生成 API 密钥和秘密。在 Umbrella 中从**管理员 (Admin)** > **API 密钥 (API Keys)** 生成密钥。生成密钥时，必须确保复制并保存 API 和密钥，因为以后无法检索密钥。密钥的范围必须是读/写。
- （旧版，不推荐。）登录 Cisco Umbrellaa 网络设备控制面板 (https://login.umbrella.com/)，获取适用于您的组织的旧版网络设备 API 令牌。此令牌是十六进制字符串，例如 AABBA59A0BDE1485C912AFE。从 Umbrella 控制面板生成旧版网络设备 API 密钥。
- 安装思科 Umbrella 注册服务器证书。

过程

步骤 1 进入 Umbrella 配置模式。

umbrella-global

示例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)#
```

步骤 2 配置向 Cisco Umbrella 注册所需的 API 密钥和秘密。

token-request-credential api-key *key_value* **secret** *secret_value*

请注意，密钥会过期，您需要禁用Umbrella，添加新密钥/秘密，并在应用新密钥时重新启用Umbrella。

示例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcbd08edc11 secret 4afe58df5c454161a10a172145cb1456
```

步骤 3 （旧版，不推荐。）配置在思科 Umbrella 中注册时所需的 API 令牌。

仅当不配置 API 密钥和秘密时，才能配置令牌。

token *api_token*

示例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE
Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
```

步骤 4 （可选。）如果想要在 DNS 检测策略映射中启用 DNScrypt DNS，则可以选择配置用于证书验证的 DNScrypt 提供商公钥。如果未配置密钥，则使用当前分布分发的默认公钥进行验证。

public-key *hex_key*

密钥是一个 32 字节的十六进制值。在 ASCII 中输入十六进制值，每个 2 字节使用一个冒号分隔符。密钥长度为 79 个字节。从思科 Umbrella 获取此密钥。

默认密钥为：
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

要恢复使用默认公钥，请输入 **no public-key**。可以省略所配置的密钥，或将其包含在 **no** 版本命令中。

示例：

```
ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
```

步骤 5 （可选。）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。

timeout edns *hh:mm:ss*

超时采用时:分:秒的格式，可以介于 0:0:0 到 1193:0:0 之间。默认值为 0:02:00（2 分钟）。

示例：

```
ciscoasa(config-umbrella)# timeout edns 00:01:00
```

步骤 6 （可选。）配置应绕过 Umbrella 的本地域名。

可以识别 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。

可以直接输入本地域名。或者，可以创建定义该域名的正则表达式，然后创建正则表达式类映射并在以下命令中指定：

local-domain-bypass {*regular_expression* | **regex class** *regex_classmap*}

示例：

```
ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# local-domain-bypass example.com
```

步骤 7 （可选。）配置您想要用于解析 DNS 请求的非默认思科 Umbrella DNS 服务器的地址。

resolver {**ipv4** | **ipv6**} *ip_address*

可以单独输入命令，以定义非默认 Umbrella 解析器的 IPv4 和 IPv6 地址。

示例：

```
ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222
ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

步骤 8 选择向 Umbrella 注册时要使用的方法

- **令牌**（旧版本，不推荐）- 在**令牌 (Token)** 字段中输入 API 令牌。
- **令牌请求凭证** - 配置以下内容：
  - **API 密钥** - 输入从 Umbrella 生成的 API 密钥。
  - **密钥** - 输入为 API 密钥提供的密钥。

在 DNS 检测策略映射中启用 Umbrella

配置全局 Umbrella 设置不足以注册设备和启用 DNS 查询重定向。必须添加 Umbrella 作为活动 DNS 检测的一部分。

可以通过将 Umbrella 添加到 preset_dns_map DNS 检测策略映射中实现全局启用 Umbrella。

但是，如果已自定义DNS检测并对不同流量类应用不同的检测策略映射，则必须在想要获取服务的每个类上启用 Umbrella。

以下程序说明如何全局实施 Umbrella。如果已自定义 DNS 策略映射，请参阅 配置 DNS 检测策略映射。

过程

步骤 1 编辑 preset_dns_map 检测策略映射，并进入参数配置模式。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)#
```

步骤 2 启用思科 Umbrella 并选择性地指定要应用于设备的思科 Umbrella 策略的名称。

umbrella ［**tag** *umbrella_policy*］［**fail-open**］

该标签为思科Umbrella中所定义策略的名称。注册期间，思科Umbrella会将策略分配到设备（如果存在策略名称）。如果未指定策略，系统将应用默认策略。

如果希望 DNS 解析在 Umbrella DNS 服务器不可用条件下运行，则请包含 **fail-open** 关键字。故障时打开的情况下，如果思科 Umbrella DNS 服务器不可用，则 Umbrella 会在该策略映射上自动禁用，并允许向系统上配置的其他 DNS 服务器发送 DNS 请求（若有）。当 DNS 服务器恢复可用状态时，策略映射会恢复使用它们。如果未包含该选项，则 DNS 请求会继续发送至无法访问的 Umbrella 解析器，因此这些请求不会收到任何回复。

示例：

```
ciscoasa(config-pmap-p)# umbrella fail-open
```

步骤 3 （可选。）启用 DNScrypt 以加密设备与思科 Umbrella 之间的连接。

dnscrypt

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。

示例：

```
ciscoasa(config-pmap-p)# dnscrypt
```

示例

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella fail-open
ciscoasa(config-pmap-p)# dnscrypt
```

验证 Umbrella 注册

在您配置全局 Umbrella 设置并在 DNS 检测中启用 Umbrella 后，设备应与思科 Umbrella 通信并进行注册。可以通过检查思科 Umbrella 是否提供了设备 ID 来检查注册是否成功。

首先，检查服务策略统计信息，查询思科 Umbrella 注册行。这应显示 Cisco Umbrella 应用的策略（标签）、连接的 HTTP 状态和设备 ID。

状态应为 200 成功。错误代码指示以下内容：401 表示 API 令牌不正确，403 表示密钥的范围不是读/写（阻止访问），405 表示 API 密钥已过期，409 表示设备已存在在 Cisco Umbrella 中部署。

如果状态为 UNKNOWN，请检查系统日志消息。信息 339011：“Umbrella API 令牌请求未收到任何响应”(Umbrella API token request received no responses) 表明在访问 api.umbrella.com 时出现了路由问题，或者您没有上传所需的证书。

请注意，Umbrella 解析器行不应指示解析器无响应。如果解析器无响应，则验证是否在访问控制策略中打开了与这些 IP 地址的 DNS 通信。这可能是临时情况，也可能表示存在路由问题。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
     Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       umbrella registration: mode: fail-open tag: default, status: 200 success, device-id:
```

```
010a13b8fbdfc9aa
         Umbrella ipv4 resolver: 208.67.220.220
         Umbrella ipv6 resolver: 2620:119:53::53
      Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
10
       DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
       DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
       DNScrypt: Certificate Update: completion 10, failure 1
```

您还可以验证运行配置（在策略映射上执行过滤）。策略映射中的 Umbrella 命令更新以显示设备 ID。当启用此命令时，无法直接配置设备 ID。以下示例编辑输出，以显示相关信息。

```
ciscoasa(config)# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
parameters
  message-length maximum client auto
  message-length maximum 512
  dnscrypt
  umbrella device-id 010a3e5760fdd6d3
  no tcp-inspection
policy-map global_policy
class inspection_default
  inspect dns preset_dns_map
```

Umbrella 连接器示例

以下主题提供 Umbrella 连接器的配置示例。

示例： 在全局 DNS 检测策略上启用 Umbrella

以下示例显示如何全局启用 Umbrella。配置使用默认公钥启用 DNScrypt。它会分配默认思科 Umbrella 企业安全策略。密钥和秘密仅为示例；您必须从 Umbrella 生成自己的有效密钥/秘密对。

此示例假设您已上传 Umbrella 注册所需的相应证书。确保下载 Umbrella 站点使用的最新根证书，因为正确的证书会随时间变化。

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcbd08edc11 secret 4afe58df5c454161a10a172145cb1456

ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella
ciscoasa(config-pmap-p)# dnscrypt
```

示例： 在使用自定义检查策略的接口上启用 Umbrella

以下示例显示如何针对特定流量类启用 Umbrella。在仅适用于 DNS/UDP 流量的内部接口上启用 Umbrella。因为我们正在启用 DNScrypt，UDP/443 必须包含在流量类中。应用名为 mypolicy（在思科 Umbrella 中定义） 的企业安全策略。密钥和秘密仅为示例；您必须从 Umbrella 生成自己的有效密钥/秘密对。

此示例假设您已上传 Umbrella 注册所需的相应证书。确保下载 Umbrella 站点使用的最新根证书，因为正确的证书会随时间变化。

```
ciscoasa(config)# dns domain-lookup outside
ciscoasa(config)# dns domain-lookup inside
ciscoasa(config)# dns name-server 208.67.220.220

ciscoasa(config)# umbrella-global
ciscoasa(config-umbrella)# token-request-credential
api-key f817feb474d94c56b3448bcbd08edc11 secret 4afe58df5c454161a10a172145cb1456


ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
ciscoasa(config-pmap-p)# dnscrypt

ciscoasa(config)# object-group service umbrella-service-object
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config-service-object-group)# service-object udp destination eq 443

ciscoasa(config)# access-list umbrella-acl extended permit
object-group umbrella-service-object any any

ciscoasa(config)# class-map dns-umbrella
ciscoasa(config-cmap)# match access-list umbrella-acl

ciscoasa(config)# policy-map inside-policy
ciscoasa(config-pmap)# class dns-umbrella
ciscoasa(config-pmap-c)# inspect dns umbrella-policy

ciscoasa(config)# service-policy inside-policy interface inside
```

示例：从 Umbrella 全局排除某些主机或网络

如果需要排除某些主机或网络使用 Umbrella，而且选择是全局性的而不是基于接口的，可以移除全局 DNS 检查，并创建单独的类来排除或包括 Umbrella 检查。

以下示例修改了全局检查策略，使 192.168.1.0/24 网络无法使用 Umbrella。

开始之前

本示例假定您已启用 DNS 并配置了 Umbrella 全局设置。

过程

步骤 1 删除全局默认 DNS 检查。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# no inspect dns
```

步骤 2 创建可启用 Umbrella 的 DNS 策略映射。

在本示例中，策略映射命名为 umbrella-policy。

```
ciscoasa(config)# policy-map type inspect dns umbrella-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# umbrella tag mypolicy
```

步骤 3 为排除在外的流量创建流量类别。

以下示例使用 ACL 来识别来自 192.168.1.0/24 网络的 UDP/53 流量。

```
ciscoasa(config)# access-list Umb_Exclude permit udp 192.168.1.0 255.255.255.0 any eq 53
ciscoasa(config)# class-map Umbrella_Exclude
ciscoasa(config-cmap)# match access-list Umb_Exclude
```

步骤 4 为应该使用 Umbrella 的主机创建流量类别。

以下示例匹配来自任何源的 UDP/53 流量。

```
ciscoasa(config)# class-map Umbrella_Include
ciscoasa(config-cmap)# match port udp eq 53
```

步骤 5 更新全局检测策略，使用适当的 DNS 策略映射为流量类别启用 DNS 检测。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)#  class Umbrella_Exclude
ciscoasa(config-pmap-c)# inspect dns
ciscoasa(config-pmap)#  class Umbrella_Include
ciscoasa(config-pmap-c)# inspect dns umbrella-policy
```

监控 Umbrella 连接器

以下主题介绍如何监控 Umbrella 连接器。

监控 Umbrella 服务策略统计信息

可以在启用 Umbrella 的情况下查看 DNS 检测的概述和详细统计信息。

show service-policy inspect dns ［**detail**］

查看所有主 DNS 检测计数器和 Umbrella 配置信息，而无需 **detail**关键字。状态字段提供系统尝试在思科 Umbrella 中注册使用的 HTTP 状态代码。

解析器行表示正在使用的 Umbrella 服务器。这些行将指出服务器是否**无响应**，或系统当前是否正在**探测**服务器以确定服务器是否可用。如果模式为故障时打开模式，系统将允许 DNS 请求转至其他 DNS 服务器 （如果配置）；否则，只要 Umbrella 服务器无响应，DNS 请求就不会收到任何响应。

```
asa(config)# show service-policy inspect dns
Interface inside:
  Service-policy: global_policy
    Class-map: inspection_default
     Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 512, drop 0
        dns-guard, count 0
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       umbrella registration: mode: fail-open tag: default, status: 200 success, device-id:
 010a13b8fbdfc9aa
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
       Umbrella: bypass 0, req inject 0 - sent 0, res recv 0 - inject 0 local-domain-bypass
 10
        DNScrypt egress: rcvd 402, encrypt 402, bypass 0, inject 402
        DNScrypt ingress: rcvd 804, decrypt 402, bypass 402, inject 402
        DNScrypt: Certificate Update: completion 10, failure 1
```

详细输出显示 DNScrypt 统计信息和使用的密钥。

```
asa(config)# show service-policy inspect dns detail
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: dnscrypt30000
      Inspect: dns dns_umbrella, packet 12, lock fail 0, drop 0, reset-drop 0,
               5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
        message-length maximum client auto, drop 0
        message-length maximum 1500, drop 0
        dns-guard, count 3
        protocol-enforcement, drop 0
        nat-rewrite, count 0
       Umbrella registration: mode: fail-open tag: default, status: 200 SUCCESS, device-id:
 010af97abf89abc3, retry 0
          Umbrella ipv4 resolver: 208.67.220.220
          Umbrella ipv6 resolver: 2620:119:53::53
       Umbrella: bypass 0, req inject 6 - sent 6, res recv 6 - inject 6 local-domain-bypass
 10
          Umbrella app-id fail, count 0
          Umbrella flow alloc fail, count 0
          Umbrella block alloc fail, count 0
          Umbrella client flow expired, count 0
          Umbrella server flow expired, count 0
          Umbrella request drop, count 0
          Umbrella response drop, count 0
        DNScrypt egress: rcvd 6, encrypt 6, bypass 0, inject 6
        DNScrypt ingress: rcvd 18, decrypt 6, bypass 12, inject 6
          DNScrypt length error, count 0
```

```
          DNScrypt add padding error, count 0
          DNScrypt encryption error, count 0
          DNScrypt magic_mismatch error, count 0
          DNScrypt disabled, count 0
          DNScrypt flow error, count 0
          DNScrypt nonce error, count 0
        DNScrypt: Certificate Update: completion 1, failure 1
          DNScrypt Receive internal drop count 0
          DNScrypt Receive on wrong channel drop count 0
          DNScrypt Receive cannot queue drop count 0
          DNScrypt No memory to create channel count 0
          DNScrypt Send no output interface count 1
          DNScrypt Send open channel failed count 0
          DNScrypt Send no handle count 0
          DNScrypt Send dupb failure count 0
          DNScrypt Create cert update no memory count 0
          DNScrypt Store cert no memory count 0
          DNScrypt Certificate invalid length count 0
          DNScrypt Certificate invalid magic count 0
          DNScrypt Certificate invalid major version count 0
          DNScrypt Certificate invalid minor version count 0
          DNScrypt Certificate invalid signature count 0
          Last Successful: 01:42:29 UTC May 2 2018, Last Failed: None
          Magic DNSC, Major Version 0x0001, Minor Version 0x0000,
          Query Magic 0x714e7a696d657555, Serial Number 1517943461,
          Start Time 1517943461 (18:57:41 UTC Feb 6 2018)
          End Time 1549479461 (18:57:41 UTC Feb 6 2019)
          Server Public Key
240B:11B7:AD02:FAC0:6285:1E88:6EAA:44E7:AE5B:AD2F:921F:9577:514D:E226:D552:6836
          Client Secret Key Hash
48DD:E6D3:C058:D063:1098:C6B4:BA6F:D8A7:F0F8:0754:40B0:AFB3:CB31:2B22:A7A4:9CEE
          Client Public key
6CB9:FA4B:4273:E10A:8A67:BA66:76A3:BFF5:2FB9:5004:CD3B:B3F2:86C1:A7EC:A0B6:1A58
          NM key Hash
9182:9F42:6C01:003C:9939:7741:1734:D199:22DF:511E:E8C9:206B:D0A3:8181:CE57:8020
```

监控 Umbrella 系统日志消息

可以监控以下 Umbrella 相关系统日志消息：

- %ASA-3-339001: DNSCRYPT certificate update failed for *number* tries.

  检查是否存在到 Umbrella 服务器的路由，以及出口接口是否启动且正常运行。此外，检查配置用于 DNScrypt 的公钥正是否正确。可能需要从思科 Umbrella 获取新密钥。

- %ASA-3-339002: Umbrella 设备注册失败，错误代码为 *error_code*。

  错误代码具有以下含义：

  - 400 - 存在请求格式或内容问题。令牌可能过短或已损坏。验证令牌与 Umbrella 控制面板上的令牌是否匹配。
  - 401 - API 令牌未授权。请尝试重新配置该令牌。如果在 Umbrella 控制面板上刷新了令牌，然后必须确保使用新令牌。
  - 409 - 设备 ID 与另一个组织存在冲突。请与 Umbrella 管理员合作检查，了解可能存在的问题。

- 500 - 内部服务器错误。与 Umbrella 管理员合作检查，了解可能存在的问题。

- %ASA-6-339003：Umbrella 设备注册成功。
- %ASA-3-339004：由于缺失令牌，Umbrella 设备注册失败。

  必须从思科 Umbrella 获取 API 令牌并将全局 Umbrella 设置中配置该令牌。
- %ASA-3-339005：经过 *number* 次尝试，Umbrella 设备注册失败。

  检查系统日志 339002 消息，以确定需要修复的错误。
- %ASA-3-339006：无法访问 Umbrella 解析器 *IP_address*，已恢复 Umbrella 重定向。

  此消息表明，系统已恢复到正常运行状态。无需任何操作。
- %ASA-3-339007：Umbrella 解析器 *IP_address* 无响应，已使用故障关闭模式，启动对解析器的探测。

  由于您正在使用故障关闭模式，因此在 Umbrella DNS 服务器重新上线前，用户不会收到有关其 DNS 请求的响应 。如果问题仍然存在，请验证是否存在从系统到 Umbrella 服务器的路由，以及在访问控制策略中是否允许 DNS 流量流向服务器。
- 与 API 密钥/密钥注册相关的消息：
  - %ASA-6-339010：Umbrella API 令牌请求成功
  - %ASA-3-339011：Umbrella API 令牌请求未收到响应
  - %ASA-3-339012：Umbrella API 令牌请求失败，错误代码为 %d
  - %ASA-3-339013：Umbrella API 令牌请求在响应处理过程中失败
  - %ASA-3-339014：Umbrella API 令牌请求在 %d 次重试后失败；中止注册

思科 Umbrella 连接器的历史记录

功能名称	平台版本	说明
思科 Umbrella 支持。	9.10(1)	您可以配置设备将 DNS 请求重定向至思科 Umbrella，以便将您在思科 Umbrella 中定义的企业安全策略应用于用户连接。您可以允许或阻止基于 FQDN 的连接，或者，对于可疑的 FQDN，您可以将用户重定向至思科 Umbrella 智能代理，该代理可以执行 URL 筛选。Umbrella 配置是 DNS 检测策略的一部分。 关键字，所以您可以显示有关特定 GTP版本的信息：**umbrella**、**umbrella-global**、**token**、**public-key**、**timeout edns**、**dnscrypt**、**show service-policy inspect dns detail**。

功能名称	平台版本	说明
思科 Umbrella 增强功能。	9.12(1)	您现在可以标识需要绕过思科 Umbrella 的本地域名。发向这些域的 DNS 请求将直接流向 DNS 服务器，而不经过 Umbrella 处理。此外，您还可以标识用于解析 DNS 请求的 Umbrella 服务器。最后，您可以定义 Umbrella 检测策略以实现故障时自动开放，以确保 Umbrella 服务器不可用时，DNS 请求不会被阻止。 添加或更改了以下命令：**local-domain-bypass**、**resolver**、**umbrella fail-open**。
新的 Umbrella API。	9.23(1)	您现在可以使用 Umbrella 开放 API 来配置 Umbrella，该 API 使用带密钥的 API 密钥。 添加了以下命令：**token-request-credential**

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。