Cisco Umbrella 統合

Cisco Umbrella 統合の前提条件

- Cisco Umbrella サブスクリプション ライセンスが利用可能である必要があります。https://umbrella.cisco.com/products/umbrella-enterprise-security-packages に移動し、[Request a quote] をクリックしてライセンスを取得します。
- デバイスはデフォルトのドメインネームシステム（DNS）サーバゲートウェイとして設定する必要があり、ドメインネームサーバのトラフィックはシスコデバイスを通過する必要があります。
- Umbrella サーバへのデバイス登録に使用する通信は HTTPS 経由です。HTTPS 通信を行うには、デバイスにルート証明書がインストールされている必要があります。次のリンクを使用して証明書をダウンロードできます。https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt
- シスコ産業用イーサネットスイッチは、Cisco IOS XE リリース 17.2.1 以降のソフトウェアイメージを実行します。
- Cisco Umbrella を有効にするには、シスコ産業用イーサネットスイッチに Cisco DNA Advantage 以上のライセンスが必要です。

次のネットワーク要件を満たす必要があります。

- デバイスをデフォルトの DNS サーバゲートウェイとして設定し、ドメインネームサーバ（DNS）トラフィックがシスコ産業用イーサネットスイッチを通過するようにします。
- Cisco Umbrella サーバへのデバイス登録に使用する通信は HTTPS 経由です。HTTPS 通信を行うには、ルータにルート証明書がインストールされている必要があります。この証明書をペーストする代わりに、次のリンクから証明書を直接ダウンロードすることができます。

  https://www.digicert.com/CACerts/DigiCertSHA2SecureServerCA.crt
- 最初の登録の場合、「umbrella out」として設定されたインターフェイスは、最初の登録を完了するために、ポート 443 を介して api.opendns.com にアクセスできる必要があります。

Cisco Umbrella 統合の制限

- Cisco Umbrella 統合は、次のシナリオでは機能しません。
  - アプリケーションまたはホストが、DNS の代わりに IP アドレスを使用してドメイン名をクエリしている場合。
  - クライアントが Web プロキシに接続されていて、サーバアドレスを解決するための DNS クエリを送信しない場合。
  - DNS クエリがシスコスイッチデバイスによって生成される場合。
  - DNS クエリが TCP 経由で送信される場合。
  - DNS クエリに、アドレスマッピングとテキスト以外のレコードタイプがある場合。
- DNSv6 クエリはサポートされていません。
- DNS64 および DNS46 拡張はサポートされていません。
- 拡張 DNS は、ホストの IPv4 アドレスのみを伝達し、IPv6 アドレスは伝達しません。
- ポートチャネルでの Cisco Umbrella 設定はサポートされていません
- Cisco Umbrella は、10G アップリンクポートを送信専用として使用するように設定できます。
- Cisco Umbrella インターフェイスを経由する DNS トラフィックの DSCP マーキングは行われません。これは、Cisco Umbrella インターフェイス上のすべてのパントされたトラフィックに適用されます。
- Cisco Umbrella インターフェイスの場合、すべての送信 ACL ルールは DNS トラフィックに影響を及ぼしません。これは、DNS の CPU 処理されるトラフィックに適用されます。
- DNS パケットのフラグメンテーションはサポートされていません。
- QinQ およびセキュリティグループタグ（SGT）パケットはサポートされていません。

- Cisco Umbrella の統合ポリシーによって DNS クエリがブロックされると、クライアントは Cisco Umbrella ブロックページにリダイレクトされます。これらのブロックページは、HTTPS サーバによって提供され、IP アドレス範囲は Cisco Umbrella ポータルによって定義されます。
- ユーザ認証とアイデンティティは、現在サポートされていません。
- Cisco Umbrella Connector は、悪意のあるトラフィックに関する既知の IP アドレスのリストを保持します。Cisco Umbrella ローミングクライアントは、これらのアドレスが宛先のパケットを検出すると、各アドレスを Cisco Umbrella クラウドに転送して、さらに検査します。
- 現在、直接クラウドアクセスはサポートされていません。
- 更新されたリゾルバ IP は有効になりません。DNS トラフィックは、ユーザが設定したリゾルバ IP に関係なく、Cisco Umbrella クラウドにリダイレクトされます。
- ネットワークアドレス変換（NAT）は、Cisco Umbrella が有効になっているインターフェイスではサポートされません。

Cisco Umbrella 統合に関する情報

ここでは、Cisco Umbrella 統合機能の詳細を説明します。

Cisco Umbrella 統合のメリット

Cisco Umbrella 統合は、DNS レベルでのセキュリティとポリシーの適用を提供します。これにより、管理者は DNS トラフィックを分割して、DNS トラフィックの一部をエンタープライズネットワーク内にある特定の DNS サーバに直接送信することができます。これにより、管理者は Cisco Umbrella 統合をバイパスできます。

Cisco Umbrella 統合を使用したクラウドベースのセキュリティサービス

Cisco Umbrella 統合機能は、Cisco デバイスを介して DNS サーバに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを提供します。ホストがトラフィックを開始し、DNS クエリを送信すると、デバイスの Cisco Umbrella コネクタは DNS クエリを横取りして検査します。Umbrella コネクタは、DNS トラフィックを横取りして、セキュリティ検査およびポリシー適用のために Cisco Umbrella クラウドへのリダイレクトを行うシスコ デバイス内のコンポーネントです。Umbrella クラウドは、Umbrella コネクタから受信したクエリを検査するクラウドベースのセキュリティサービスであり、完全修飾ドメイン名（FQDN）に基づいて、コンテンツプロバイダーの IP アドレスを応答に含めるかどうかを決定します。

ローカルドメインへの DNS クエリの場合、DNS パケットを変更せずに企業ネットワーク内の DNS サーバにクエリが転送されます。Cisco Umbrella リゾルバは、外部ドメインから送信され

た DNS クエリを検査します。デバイス ID 情報、組織 ID、クライアント IP アドレスを含む拡張 DNS レコードがクエリに追加され、Cisco Umbrella リゾルバに送信されます。Umbrella クラウドは、このすべての情報に基づいて、DNS クエリにさまざまなポリシーを適用します。

Umbrella 統合クラウドは、ポータルで設定されたポリシーと DNS FQDN のレピュテーションに基づいて、次のいずれかのアクションを実行します。

- ブラックリストのアクション：FQDN が悪意のあるものであるか、カスタマイズされたエンタープライズセキュリティポリシーによってブロックされていると判明した場合、Cisco Umbrella クラウドのブロックランディングページの IP アドレスが DNS 応答で返されます。
- ホワイトリストのアクション：FQDN が悪意のないものであると判明した場合、コンテンツプロバイダーの IP アドレスが DNS 応答で返されます。
- グレーリストのアクション：FQDN が疑わしいと判明した場合、インテリジェントプロキシのユニキャスト IP アドレスが DNS 応答で返されます。

DNS 応答を受信すると、デバイスは応答をホストに転送します。ホストは応答から IP アドレスを抽出し、HTTP または HTTPS 要求をこの IP アドレスに送信します。

Cisco Umbrella クラウドによるトラフィックの処理

Cisco Umbrella 統合機能を使用すると、HTTP および HTTPS クライアント要求は次のように処理されます。

- DNS クエリの FQDN が悪意のあるものである場合（ブラックリストに登録されたドメインに含まれる場合）、Cisco Umbrella クラウドは DNS 応答でブロック時用ランディングページの IP アドレスを返します。HTTP クライアントがこの IP アドレスに要求を送信すると、Umbrella クラウドは、要求されたページがブロックされたことをユーザに通知するページと、ブロックの理由を表示します。
- DNS クエリの FQDN が悪意のないものである場合（ホワイトリストに登録されたドメインに含まれる場合）、Cisco Umbrella クラウドはコンテンツプロバイダーの IP アドレスを返します。HTTP クライアントはこの IP アドレスに要求を送信し、要求されたコンテンツを取得します。
- DNS クエリの FQDN がグレーリストのドメインに該当する場合、Umbrella DNS リゾルバは DNS 応答でインテリジェントプロキシのユニキャスト IP アドレスを返します。ホストからグレードメインへのすべての HTTP トラフィックは、インテリジェントプロキシを介してプロキシされ、Uniform Resource Locator（URL）フィルタリングが実行されます。

（注） インテリジェントプロキシのユニキャスト IP アドレスを使用する場合の潜在的な制限の 1 つは、クライアントがインテリジェントプロキシのユニキャスト IP アドレスにトラフィックを送信しようとしたときにデータセンターがダウンする可能性です。このシナリオでは、クライアントはグレーリストのドメインに該当するドメインの DNS 解決を完了し、クライアントの HTTP または HTTPS トラフィックは、取得されたインテリジェントプロキシのユニキャスト IP アドレスのいずれかに送信されます。そのデータセンターがダウンしている場合、クライアントはそれを知る方法がありません。

Umbrella コネクタは、HTTP および HTTPS トラフィックに対して動作しません。コネクタは、Web トラフィックをリダイレクトしたり、HTTP または HTTPS パケットを変更したりしません。

DNS パケット暗号化

Cisco デバイスから Cisco Umbrella 統合サーバに送信される DNS パケットは、パケット内の拡張 DNS 情報にユーザ ID、内部ネットワーク IP アドレスなどの情報が含まれている場合、暗号化する必要があります。DNS 応答が DNS サーバから戻されると、デバイスはパケットを復号化してからホストに転送します。

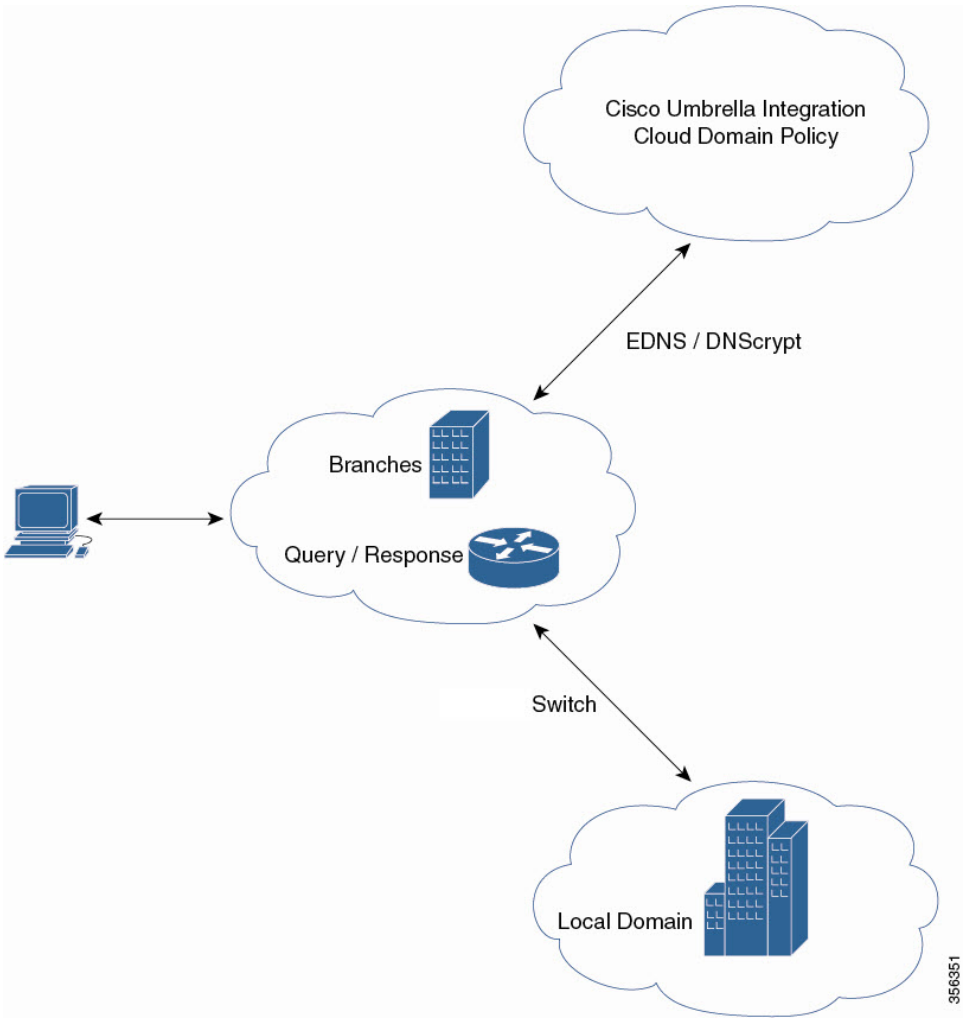
（注）
- DNS パケットは、DNScrypt 機能が Cisco デバイスで有効化されている場合にのみ暗号化できます。
- 統計情報を追跡するために、クライアントの IP アドレスが Umbrella クラウドにエクスポートされます。IP は暗号化されずに送信されるため、DNScrypt を無効にしないことを推奨します。

Cisco デバイスは次の Anycast 再帰型 Cisco Umbrella 統合サーバを使用します。

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

次の図に、Cisco Umbrella 統合のトポロジを示します。

図 *1 : Cisco Umbrella* 統合のトポロジ



DNSCrypt と公開キー

次のサブセクションでは、DNScrypt と公開キーについて詳しく説明します。

DNSCrypt

DNSCrypt は、Cisco デバイスと Cisco Umbrella 統合機能間の通信を認証する暗号化プロトコルです。**parameter-map type umbrella** が設定され、WAN インターフェイスで **umbrella out** コマンドが有効化されると、DNSCrypt がトリガーされ、証明書のダウンロード、検証、解析が行われます。次に、DNS クエリの暗号化に使用される共有秘密鍵のネゴシエーションが行われます。一時間おきにこの証明書が自動的にダウンロードされ、アップグレードのために検証され、その都度新しい共有秘密キーがネゴシエートされ、DNS クエリが暗号化されます。

DNSCrypt を使用する場合は、DNS 要求パケットサイズが 512 バイトよりも大きくなります。これらのパケットが中間デバイスを通過できることを確認します。そうしないと、応答が目的の受信者に到達しない可能性があります。

公開キー

公開キーは、Umbrella クラウドから DNSCrypt 証明書をダウンロードするために使用されます。この値は、B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79（Cisco Umbrella Integration Anycast サーバの公開キー）に事前に設定されています。公開キーに変更があり、**public-key** コマンドを変更する場合、デフォルト値に戻すときは変更されたコマンドを削除する必要があります。

⚠

注意 この値を変更すると、DNSCrypt 証明書のダウンロードは失敗することがあります。

parameter-map type umbrella global コマンドは、Umbrella モードでパラメータマップタイプを設定します。このコマンドを使用してデバイスを設定すると、DNSCrypt と公開キーの値が自動入力されます。

ラボで特定のテストを実行するときは、**parameter-map type umbrella global** パラメータのみを変更することをお勧めします。これらのパラメータを変更すると、デバイスの正常な機能に影響が及ぶことがあります。

Cisco Umbrella 統合の設定方法

ここでは、Cisco Umbrella 統合を構成するさまざまな作業について説明します。

Umbrella Connector の設定

Before you begin

Cisco Umbrella 登録サーバからアプリケーションプログラミングインターフェイス（API）トークンを取得します。

Cisco Umbrella 登録サーバとの間で HTTPS 接続を確立するために、ルート証明書を取得します。グローバル コンフィギュレーション モードで **crypto pki trustpool import terminal** コマンドを使用して、DigiCert のルート証明書をデバイスにインポートします。

証明書をインポートする方法は 2 つあります。

1. URL からインポートする
2. 端末で直接インポートする

URL からインポートするには、コマンドを発行し、産業用イーサネットスイッチが証明書を取得できるようにします。

crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b

端末からインポートするには、次の手順を実行します。

DigiCert のルート証明書は次のとおりです。

```
-----BEGIN CERTIFICATE-----
MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kTANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xMzAzMDgxMjAwMDBaFw0yMzAzMDgxMjAwMDBaME0xCzAJBgNVBAYTAlVT
MRUwEwYDVQQKEwxEaWdpQ2VydCBJbmMxJzAlBgNVBAMTHkRpZ2lDZXJ0IFNIQTIg
U2VjdXJlIFNlcnZlciBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
ANyuWJBNwcQwFZA1W248ghX1LFy949v/cUP6ZCWA1O4Yok3wZtAKc24RmDYXZK83
nf36QYSvx6+M/hpzTc8zl5CilodTgyu5pnVILR1WN3vaMTIa16yrBvSqXUu3R0bd
KpPDkC55gIDvEwRqFDu1m5K+wgdlTvza/P96rtxcflUxDOg5B6TXvi/TC2rSsd9f
/ld0Uzs1gN2ujkSYs58O09rg1/RrKatEp0tYhG2SS4HD2nOLEpdIkARFdRrdNzGX
kujNVA075ME/OV4uuPNcfhCOhkEAjUVmR7ChZc6gqikJTvOX6+guqw9ypzAO+sf0
/RR3w6RbKFfCs/mC/bdFWJsCAwEAAaOCAVowggFWMBIGA1UdEwEB/wQIMAYBAf8C
AQAwDgYDVR0PAQH/BAQDAgGGMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYY
aHR0cDovL29jc3AuZGlnaWNlcnQuY29tMHsGA1UdHwR0MHIwN6A1oDOGMWh0dHA6
Ly9jcmwzLmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwN6A1
oDOGMWh0dHA6Ly9jcmw0LmRpZ2ljZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RD
QS5jcmwwPQYDVR0gBDYwNDAyBgRVHSAAMCowKAYIKwYBBQUHAgEWHGh0dHBzOi8v
d3d3LmRpZ2ljZXJ0LmNvbS9DUFMwHQYDVR0OBBYEFA+AYRyCMWHVLyjnjUY4tCzh
xtniMB8GA1UdIwQYMBaAFAPeUDVW0Uy7ZvCj4hsbw5eyPdFVMA0GCSqGSIb3DQEB
CwUAA4IBAQAjPt9L0jFCpbZ+QlwaRMxp0Wi0XUvgBCFsS+JtzLHgl4+mUwnNqipl
5TlPHoOlblyYoiQm5vuh7ZPHLgLGTUq/sELfeNqzqPlt/yGFUzZgTHbO7Djc1lGA
8MXW5dRNJ2Srm8c+cftIl7gzbckTB+6WohsYFfZcTEDts8Ls/3HB40f/1LkAtDdC
2iDJ6m6K7hQGrn2iWZiIqBtvLfTyyRRfJs8sjX7tN8Cp1Tm5gr8ZDOo0rwAhaPit
c+LJMto4JQtV05od8GiG7S5BNO98pVAdvzr508EIDObtHopYJeS4d60tbvVS3bR0
j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz
-----END CERTIFICATE-----
```

プライバシー強化メール（PEM）インポートが正常に行われたことを確認します。証明書をインポートすると、確認メッセージが表示されます。

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type umbrella global**
4. **dnscrypt**
5. **token** *value*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。

	Command or Action	Purpose
ステップ 2	**configure terminal** **Example:** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	パラメータマップタイプを umbrella モードに設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 4	**dnscrypt** **Example:** `Device(config-profile)# dnscrypt`	デバイスで DNS パケット暗号化を有効にします。
ステップ 5	**token** *value* **Example:** `Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC`	Cisco Umbrella 登録サーバによって発行された API トークンを指定します。
ステップ 6	**end** **Example:** `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Cisco Umbrella タグの登録

Before you begin

- Umbrella Connector を設定します。
- **umbrella in** コマンドを設定する前に **umbrella out** コマンドを設定します。登録は、ポート 443 がオープン状態にあり、既存のファイアウォールへのトラフィックのパススルーが許可される場合にのみ成功します。
- タグを指定して **umbrella in** コマンドを設定すると、デバイスは api.opendns.com を解決して登録プロセスを開始します。**ip name-server** コマンドを使用してネームサーバを設定し、デバイスで設定された **ip domain-lookup** コマンドを使用してドメインルックアップを設定して、FQDN を正常に解決します。

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **umbrella out**
5. **exit**
6. **interface** *interface-type interface-number*
7. **umbrella in** *tag-name*
8. **end**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** **Example:** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitEthernet 1/1`	WAN インターフェイスを指定して、インターフェイス コンフィギュレーションモードを開始します。
ステップ 4	**umbrella out** **Example:** `Device(config-if)# umbrella out`	Umbrella クラウドサーバに接続するためのインターフェイスで Umbrella Connector を設定します。
ステップ 5	**exit** **Example:** `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーションモードを開始します。
ステップ 6	**interface** *interface-type interface-number* **Example:** `Device(config)# interface gigabitEthernet 1/2`	LAN インターフェイスを指定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 7	**umbrella in** *tag-name* **Example:**	クライアントに接続されているインターフェイスで Umbrella Connector を設定します。

	Command or Action	Purpose
	`Device(config-if)# umbrella in mydevice_tag`	• Umbrella タグの長さは 49 文字までです。 • タグを使用して **umbrella in** コマンドを設定すると、デバイスは Cisco Umbrella 統合サーバにタグを登録します。
ステップ 8	**end** **Example:** `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

Cisco デバイスをパススルーサーバとして設定

ドメイン名を使用して、バイパスされるトラフィックを特定することができます。Cisco デバイスでは、正規表現形式でこれらのドメインを定義できます。デバイスによって横取りされた DNS クエリが、設定済みの正規表現の 1 つにマッチすると、このクエリは、Umbrella クラウドにリダイレクトされずに、指定された DNS サーバにバイパスされます。

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **parameter-map type regex** *parameter-map-name*
4. **pattern** *expression*
5. **exit**
6. **parameter-map type umbrella global**
7. **token** *value*
8. **local-domain** *regex_param_map_name*
9. **end**

DETAILED STEPS

	Command or Action	Purpose
ステップ 1	**enable** **Example:** `Device> enable`	特権 EXEC モードを有効にします。プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** **Example:** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	Command or Action	Purpose
ステップ 3	**parameter-map type regex** *parameter-map-name* **Example:** `Device(config)# parameter-map type regex dns_bypass`	パラメータマップタイプを指定されたトラフィックパターンに一致するように設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。

ステップ 4	**pattern** *expression*
	Example:
	`Device(config-profile)# pattern www.cisco.com`
	`Device(config-profile)# pattern .*example.cisco.*`
		Umbrella クラウドをバイパスするために使用するローカルドメインまたは URL を設定します。

ステップ 5	**exit** **Example:** `Device(config-profile)# exit`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 6	**parameter-map type umbrella global** **Example:** `Device(config)# parameter-map type umbrella global`	パラメータマップタイプを umbrella モードに設定し、パラメータマップタイプ検査コンフィギュレーション モードを開始します。
ステップ 7	**token** *value* **Example:** `Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF`	Cisco Umbrella 登録サーバによって発行された API トークンを指定します。
ステップ 8	**local-domain** *regex_param_map_name* **Example:** `Device(config-profile)# local-domain dns_bypass`	正規表現パラメータマップを Umbrella グローバル コンフィギュレーションにアタッチします。
ステップ 9	**end** **Example:** `Device(config-profile)# end`	パラメータ マップ タイプ検査コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

Cisco Umbrella 統合の設定の確認

Cisco Umbrella 統合の設定を表示および確認するには、次のコマンドを任意の順序で使用します。

次に、**show umbrella config** コマンドの出力例を示します。

```
Device# show umbrella config
Umbrella Configuration
=======================
Token: EB74330C50767B6A63770EA6C3408DCF00282D8E
API-KEY: NONE
OrganizationID: 2633102
Local Domain Regex parameter-map name: NONE
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
UDP Timeout: 5 seconds
Resolver address:
1. 208.67.220.220
2. 208.67.222.222
3. 2620:119:53::53
4. 2620:119:35::35
Umbrella Interface Config:
Number of interfaces with "umbrella out" config: 1
1. GigabitEthernet1/4
Mode : OUT
VRF : global(Id: 0)
Number of interfaces with "umbrella in" config: 2
1. GigabitEthernet1/9
Mode : IN
DCA : Disabled
Tag : IE_uniquetag
Device-id : 010a424c1597fe09
VRF : global(Id: 0)
2. GigabitEthernet2/3
Mode : IN
DCA : Disabled
Tag : IE_tag_2
Device-id : 010adaf012a36ad6
VRF : global(Id: 0)
Configured Umbrella Parameter-maps:
1. global
```

次に、**show umbrella deviceid** コマンドの出力例を示します。

```
Device# show umbrella deviceid

Device registration details
Interface Name Tag Status Device-id
GigabitEthernet1/9 IE_uniquetag 200 SUCCESS 010a424c1597fe09
GigabitEthernet2/3 IE_tag_2 200 SUCCESS 010adaf012a36ad6
```

次に、**show umbrella dnscrypt** コマンドの出力例を示します。

```
Device#show umbrella dnscrypt
DNSCrypt: Enabled
Public-key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79
Certificate Update Status:
Last Successfull Attempt: 20:01:18 IST Dec 17 2019
```

```
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x7163373861576F6F
Serial Number : 1574811744
Start Time : 1574811744 (05:12:24 IST Nov 27 2019)
End Time : 1606347744 (05:12:24 IST Nov 26 2020)
Server Public Key :
88B4:E44B:35E9:64B4:90BD:DABA:E825:A24B:0415:A08B:E19D:7DDB:87A3:3CD7:7EDF:8E2F
Client Secret Key Hash:
0FB9:520E:5228:FB2C:D521:1E9E:2ACB:AC3D:B520:A795:F54C:C608:604B:A410:17F1:1284
Client Public key :
E42F:507E:F052:72DD:1BC8:4857:2AE0:2F9F:ED87:1687:AAE4:095D:D933:48F0:5D60:3662
NM key Hash :
EDC3:25DD:4D21:103E:7E49:1EFA:75ED:4D6F:A450:107D:C6E8:1C41:9CF7:4039:FA89:2CED
```

次に、**show umbrella deviceid detailed** コマンドの出力例を示します。

```
Device# show umbrella deviceid detailed

Device registration details
1.GigabitEthernet1/9
Tag : IE_uniquetag
Device-id : 010a424c1597fe09
Description : Device Id recieved successfully
WAN interface : GigabitEthernet1/4
WAN VRF used : global(Id: 0)
2.GigabitEthernet2/3
Tag : IE_tag_2
Device-id : 010adaf012a36ad6
Description : Device Id recieved successfully
WAN interface : GigabitEthernet1/4
WAN VRF used : global(Id: 0)
```

次に、**show platform software dns-umbrella statistics** コマンドの出力例を示します。コマンド出力には、送信されたクエリの数、受信した応答の数などのトラフィック関連の情報が表示されます。

```
Device# show platform software dns-umbrella statistics

=======================================
Umbrella Statistics
=======================================
Total Packets : 7848
DNSCrypt queries : 3940
DNSCrypt responses : 0
DNS queries : 0
DNS bypassed queries(Regex) : 0
DNS responses(Umbrella) : 0
DNS responses(Other) : 3906
Aged queries : 34
Dropped pkts : 0
```

Cisco Umbrella 統合のトラブルシューティング

次のコマンドを使用して、Cisco Umbrella 統合機能の設定に関連する問題をトラブルシューティングできます。

表 *1 : Cisco Umbrella* 統合機能のデバッグコマンド

コマンド	目的
debug umbrella config	Umbrella 設定のデバッグを有効にします。
debug umbrella device-registration	Umbrella デバイス登録のデバッグを有効にします。
debug umbrella dnscrypt	Umbrella DNSCrypt 暗号化のデバッグを有効にします。

Windows マシンのコマンドプロンプト、または Linux マシンのターミナルウィンドウもしくはシェルから、**nslookup -type=txt debug.opendns.com** コマンドを実行します。**nslookup -type=txt debug.opendns.com** コマンドで指定する IP アドレスは、DNS サーバの IP アドレスである必要があります。

```
nslookup -type=txt debug.opendns.com 10.0.0.1
Server: 10.0.0.1
Address: 10.0.0.1#53
Non-authoritative answer:
debug.opendns.com text = "server r6.xx"
debug.opendns.com text = "device 010A826AAABB6C3D"
debug.opendns.com text = "organization id 1892929"
debug.opendns.com text = "remoteip 10.0.1.1"
debug.opendns.com text = "flags 436 0 6040 39FF000000000000000"
debug.opendns.com text = "originid 119211936"
debug.opendns.com text = "orgid 1892929"
debug.opendns.com text = "orgflags 3"
debug.opendns.com text = "actype 0"
debug.opendns.com text = "bundle 365396"
debug.opendns.com text = "source 10.1.1.1:36914"
debug.opendns.com text = "dnscrypt enabled (713156774457306E)"
```

Cisco Umbrella 統合の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

表 *2 : Cisco Umbrella* 統合の機能情報

機能名	リリース	機能情報
Cisco Umbrella 統合	Cisco IOS XE Amsterdam 17.2.1	Cisco Umbrella 統合機能により、Cisco デバイスを介して任意の DNS サーバに送信される DNS クエリを検査する、クラウドベースのセキュリティサービスを利用できるようになります。セキュリティ管理者は、FQDN へのトラフィックを許可または拒否するポリシーを Cisco Umbrella クラウドに設定します。