Cisco Umbrella 統合の設定

Cisco Umbrella 統合機能では、デバイスを介して DNS サーバーに送信されるドメインネームシステム（DNS）クエリを検証して、クラウドベースのセキュリティサービスを有効にすることができます。セキュリティ管理者は、完全修飾ドメイン名（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 ポータルに設定します。Cisco スイッチは、ネットワークエッジの DNS フォワーダとして機能し、DNS トラフィックを透過的にキャッチして Cisco Umbrella ポータルに DNS クエリを転送します。

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/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。
- Umbrella サーバー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

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 Cisco Catalyst デバイスによって生成された場合。
  - 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。
- 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。
- **umbrella in** コマンドと **umbrella out** コマンドを同じインターフェイスで設定することはできません。これらのコマンドはどちらも管理インターフェイスではサポートされておらず、ポート単位でのみ設定できます。
- 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 Active Directory 統合では、ユーザーが正常に認証される前にインターフェイスで **umbrella in** コマンドが有効になっていない場合、ユーザー名情報は DNS クエリとともに送信されず、デフォルトのグローバルポリシーがそのような DNS クエリに適用されることがあります。
- Cisco Umbrella の登録およびリダイレクトは、グローバル Virtual Routing and Forwarding（VRF）でのみ実行できます。他の VRF を介した Umbrella サーバーへの接続はサポートされていません。
- Cisco Umbrella コンフィギュレーション コマンドは、L2 および L3 物理ポートでのみ設定でき、ポートチャネルやスイッチ仮想インターフェイス（SVI）などの他のインターフェイスでは設定できません。SVI では、Umbrella サーバーへの接続に Umbrella 設定コマンドは必要ありません。

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 サーバーに送信される 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 サーバー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、およびクライアントユーザー名（ハッシュ形式）を含む拡張 DNS レコードがクエリに追加され、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。

Cisco Umbrella Active Directory コネクタは、オンプレミスの Active Directory から Umbrella リゾルバへのユーザー情報マッピングとグループ情報マッピングを、定期的に取得してアップロードします。Umbrella リゾルバですべてのユーザーとグループの事前にアップロードされたレコードに基づいて、Umbrella クラウドは受信した DNS パケットに適切なポリシーを適用します。Cisco Umbrella Active Directory コネクタのインストール方法の詳細については、『Active Directory Setup Guide』を参照してください。

（注）

- Cisco Umbrella Active Directory 統合は、デバイスで Umbrella コネクタが有効で、動作するために追加のコマンドを必要としない場合、デフォルトで設定されます。
- Umbrella コネクタは、ポートベースの認証プロセスから自動的にユーザー名を取得し、ユーザーが送信するすべての DNS クエリにユーザー名を追加します。ポートベースの認証プロセスについては、「*IEEE 802.1x* ポートベース認証の設定」の章を参照してください。

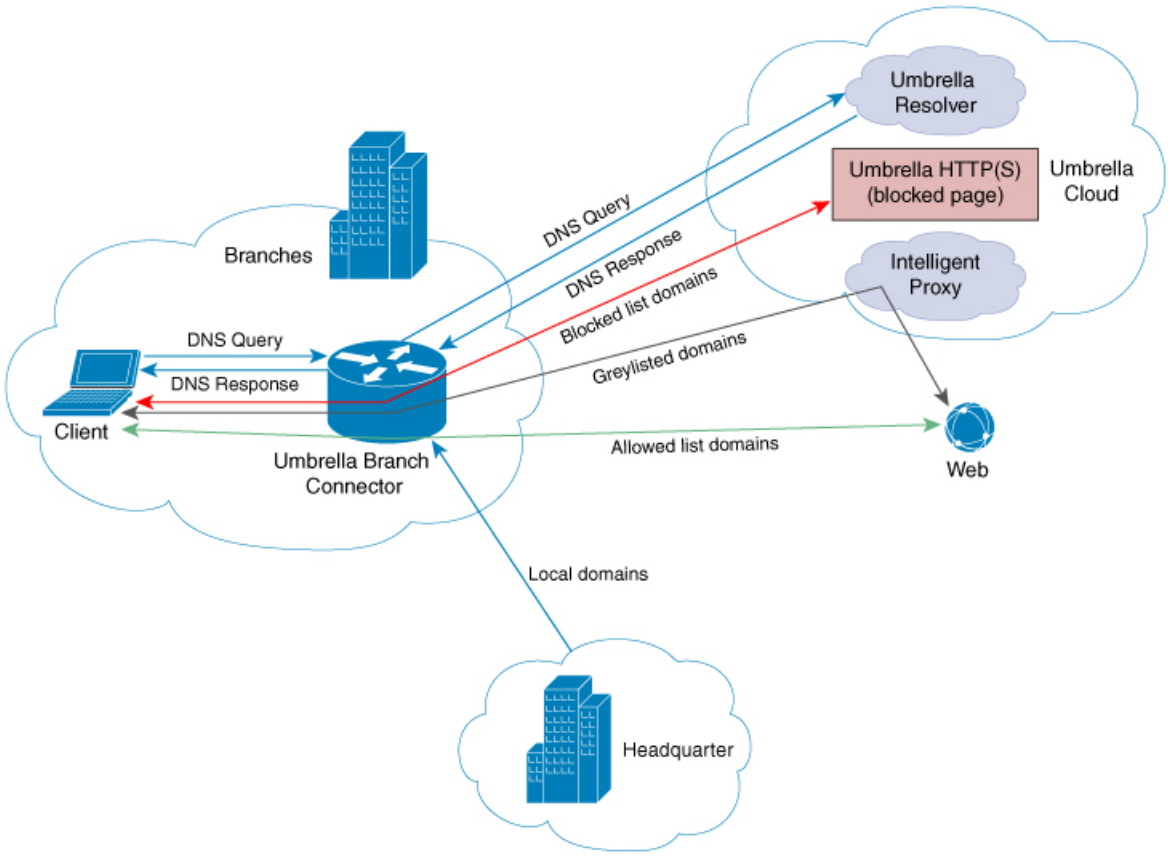
Cisco Identity Services Engine（ISE）は、ネットワークリソースへのセキュアなアクセスを提供するセキュリティポリシー管理プラットフォームです。Cisco Umbrella Active Directory コネクタが動作するには、Cisco ISE のサポートが必須です。この統合の動作の詳細については、「Active Directory Integration with Cisco ISE 2.x」を参照してください。

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。

- ブロ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、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。
- 許可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。

次の図は、Umbrella コネクタと Umbrella クラウド間のトラフィックフローを示しています。

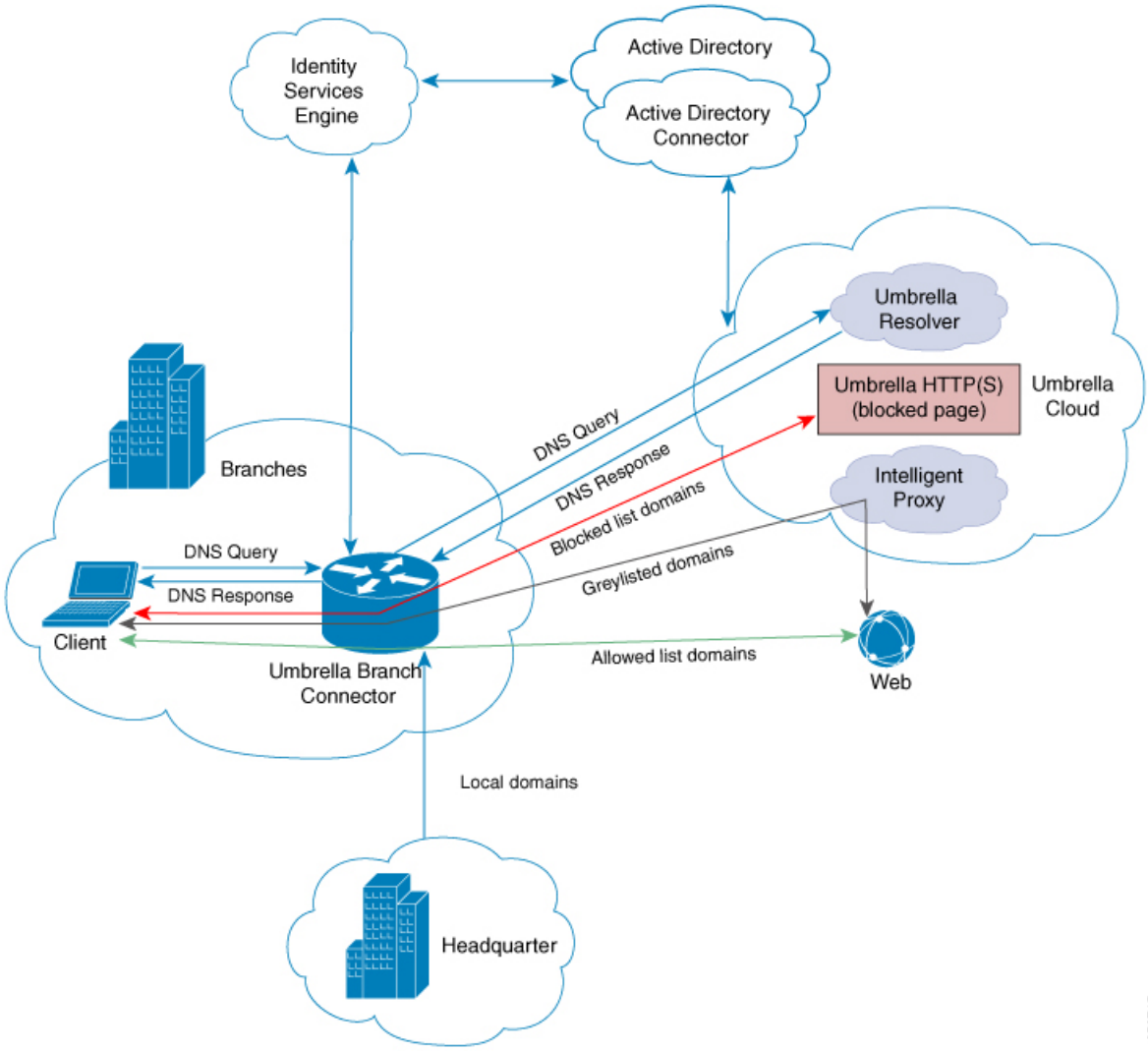
図 *1 : Cisco Umbrella* 統合を使用したクラウドベースのセキュリティサービス



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。

次の図は、Umbrella コネクタ、Cisco Identity Services Engine、Umbrella Active Directory コネクタ、および Umbrella クラウド間のトラフィックフローを示しています。

図 *2 : 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 Identity Services Engine* と *Umbrella Active Directory* コネクタを使用）



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（ブロックされているドメインのリストに含まれる場合）、Umbrella クラウドは DNS 応答でブロックされた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、リクエストされたページがブロックされた理由とともにユーザーに通知するページを表示します。

- DNS クエリの FQDN が悪意のないものである場合（許可されているドメインのリストに含まれる場合）、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、URL フィルタリングを受けます。

（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 Connector は、HTTP および HTTPS トラフィックに作用したり、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することはありません。

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。

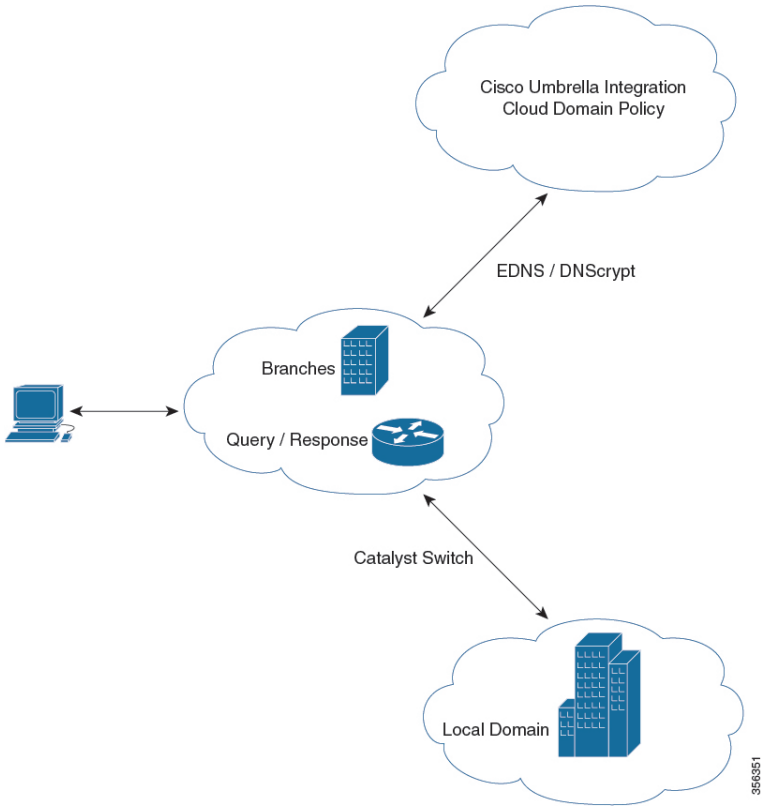
（注）
- DNS パケットは、DNScrypt 機能が Cisco デバイスで有効化されている場合にのみ暗号化できます。
- 統計情報を追跡するために、クライアントの IP アドレスが Umbrella クラウドにエクスポートされます。IP が暗号化されずに送信されるため、DNScrypt を無効にしないことをお勧めします。

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

次の図に、Cisco Umbrella 統合のトポロジを示します。

図 *3 : 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。

デバイスで DNSCrypt を有効にすると、すべての DNS トラフィックが暗号化されます。その後、DNS トラフィック インスペクションがアップストリーム ファイアウォール（この場合は Cisco 適応型セキュリティアプライアンス（ASA）ファイアウォール）で有効になっている場合、暗号化されたトラフィックは検査できません。この結果、DNSパケットがファイアウォールによってドロップされ、DNS解決に失敗する可能性があります。これを回避するには、アッ

プストリーム ファイアウォールで DNS トラフィック インスペクションを無効にする必要があります。Cisco適応型セキュリティアプライアンス（ASA）ファイアウォールでDNS トラフィック インスペクションを無効にする方法については、『Cisco ASA Series Firewall CLI Configuration Guide』を参照してください。

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 サーバーの公開キー）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 のタグ

Cisco Umbrella タグは、インターフェイスで Cisco Umbrella コネクタを設定するために使用されます。Umbrella ダッシュボードを使用して、Umbrella タグを特定の DNS ポリシーに適用できます。これらの DNS ポリシーは、タグ名がポリシー名と一致する限り Umbrella タグに自動的に適用され、指定されたインターフェイスを介して接続されているクライアントにのみ適用されます。Umbrella サーバーでポリシーと関連オプションを作成する方法については、https://docs.umbrella.com/deployment-umbrella/docs/customize-your-policies-1 を参照してください。

（注）
- すべてのインターフェイスが同じ Umbrella タグを使用して、統一ポリシーを形成できます。したがって、各インターフェイスに固有の Umbrella タグは必要ありません。
- Umbrella タグに対応するポリシーが Umbrella サーバーにない場合、タグは自動的にデフォルトでそのサーバーのグローバルポリシーに戻ります。

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

始める前に

- 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。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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**parameter-map type umbrella global** 例： `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** 例： `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* 例： `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** 例： `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

始める前に

- 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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** 例： `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* 例： `Device(config)# interface gigabitEthernet 1/0/1`	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** 例： `Device(config-if)# umbrella out`	Umbrella クラウドサーバーに接続するためにインターフェイスで Umbrella Connector を設定します。
ステップ 5	**exit** 例： `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* 例： `Device(config)# interface gigabitEthernet 1/0/2`	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* 例： `Device(config-if)# umbrella in mydevice_tag`	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。 • 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。

	コマンドまたはアクション	目的
ステップ 8	**end** 例： `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ーとして設定

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。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `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** 例： `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 regex** *parameter-map-name* 例： `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*
	例：
	`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。

	コマンドまたはアクション	目的
ステップ 5	**exit** 例： `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** 例： `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* 例： `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* 例： `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** 例： `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 統合の設定例

次のセクションに Umbrella 統合の設定例を示します。

例：Cisco Umbrella 統合の設定

次に、Umbrella コネクタを設定し、Umbrella タグを登録する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type umbrella global
Device(config-profile)# dnscrypt
Device(config-profile)# token AABBA59A0BDE1485C912AFE472952641001EEECC
Device(config-profile)# exit
Device(config)# interface GigabitEthernet 1/0/1
```

```
Device(config-if)# umbrella out
Device(config-if)# exit
Device(config)# interface gigabitEthernet 1/0/2
Device(config-if)# umbrella in mydevice_tag
Device(config-if)# exit
```

例：Cisco デバイスをパススルーサーバーとして設定

次に、Cisco デバイスをパススルーサーバーとして設定する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type regex dns_bypass
Device(config-profile)# pattern www.cisco.com
Device(config-profile)# exit
Device(config)# parameter-map type umbrella global
Device(config-profile)# token AADDD5FF6E510B28921A20C9B98EEEFF
Device(config-profile)# local-domain dns_bypass
Device(config-profile)# end
```

Cisco Umbrella 統合の設定の確認

Cisco Umbrella 統合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: 0C6ED7E376DD4D2E04492CE7EDFF1A7C00250986
   API-KEY: NONE
   OrganizationID: 2427270
   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. GigabitEthernet1/0/48
             Mode     :  OUT
             VRF      : global(Id: 0)
       Number of interfaces with "umbrella in" config: 1
         1. GigabitEthernet1/0/1
             Mode       : IN
             DCA        : Disabled
             Tag        : test
             Device-id  : 010a2c41b8ab019c
             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
GigabitEthernet1/0/1    guest           200 SUCCESS     010a2c41b8ab019c
```

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 Successful Attempt : 10:55:40 UTC Apr 14 2016
Last Failed Attempt : 10:55:10 UTC Apr 14 2016
Certificate Details:
Certificate Magic : DNSC
Major Version : 0x0001
Minor Version : 0x0000
Query Magic : 0x717744506545635A
Serial Number : 1435874751
Start Time : 1435874751 (22:05:51 UTC Jul 2 2015)
End Time : 1467410751 (22:05:51 UTC Jul 1 2016)
Server Public Key :
ABA1:F000:D394:8045:672D:73E0:EAE6:F181:19D0:2A62:3791:EFAD:B04E:40B7:B6F9:C40B
Client Secret Key Hash :
BBC3:409F:5CB5:C3F3:06BD:A385:78DA:4CED:62BC:3985:1C41:BCCE:1342:DF13:B71E:F4CF
Client Public key :
ECE2:8295:2157:6797:6BE2:C563:A5A9:C5FC:C20D:ADAF:EB3C:A1A2:C09A:40AD:CAEA:FF76
NM key Hash :
F9C2:2C2C:330A:1972:D484:4DD8:8E5C:71FF:6775:53A7:0344:5484:B78D:01B1:B938:E884
```

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.GigabitEthernet1/0/2
      Tag               : guest
      Device-id         : 010a6aef0b443f0f
      Description       : Device Id received successfully
      WAN interface     : GigabitEthernet1/0/1
      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。
debug umbrella redundancy	Umbrella 冗長性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 統合の追加情報

関連資料

関連項目	マニュアル タイトル
セキュリティ コマンド	Cisco IOS XE Amsterdam 17.1.x（Catalyst 9300 スイッチ）コマンドリファレンス

Cisco Umbrella 統合の機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Amsterdam 17.1.1	Cisco Umbrella 統合	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。
Cisco IOS XE Amsterdam 17.3.1	Umbrella Connector の Active Directory 統合	Active Directory コネクタは、ユーザーとグループのマッピングを定期的に取得して、オンプレミスの Active Directory から Umbrella Resolver にアップロードします。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn [英語] からアクセスします。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。